Guido Travaini, Chiara Mellace

Considerazioni criminologiche sull'*aging care*. Rassegna degli studi tra opportunità e rischi

1. Premessa

L'invecchiamento demografico rappresenta una sfida per la società contemporanea. Cresce il numero di persone con età superiore a 65 anni (DESA 2019) e parallelamente si va riducendo il tasso di fertilità, con una crescita significativa di famiglie mononucleari (Freedman 1996; Pearce *et al*. 1999; Krug *et al.* 2002; Congzhi, Jingzhong 2014; Grinin, Korotayev 2016). Inoltre, si riscontra una significativa sofferenza dei sistemi sanitari che si caratterizzano per una documentata carenza di organico (Haddad 2019; Scheffler *et al.* 2016; Liu *et al*. 2017; OECD 2019; van Kemenade *et al.* 2015; Coughlin *et al*. 2006; Fujisawa, Colombo 2009; Murray 2002)[1].

Tutto ciò non potrà che avere, e in parte già ha, una serie di ripercussioni negative sulla capacità di assistenza che saranno enfatizzate nell'ambito del *caregiving* per le fasce di età più bisognose (Shu-Chuan, Sing Kai 2004; Golden *et al.* 2009; Arslantaş *et al.* 2015; Dury, 2014; Landeiro *et al.* 2017).

[1] La *World Health Organization* ha previsto per il 2030 una carenza a livello di personale sanitario di 18 milioni di unità, descrivendo il dato come una "crisi globale" (*WHO Draft global strategy on human resources for health: workforce 2030*, aprile 2016). Una amara parentesi va inoltre aperta in merito alla situazione italiana. Già da tempo era stato attestato un bilancio negativo per le professioni nel Sistema Sanitario Nazionale. In particolare, è stata segnalata una riduzione del personale sanitario media pari al 6,6 per cento, prendendo in esame Aziende USL, ospedaliere e regionali (per i dati si è fatto riferimento al Rapporto Sanità, 2019 redatto da Nebo Ricerche PA). Questo calo e il conseguente sottorganico hanno tristemente fatto sentire il loro peso in questi giorni in cui ci si trova a dover fare fronte a un'importante emergenza sanitaria.

Biblioteca della libertà, LV, 2020
settembre-dicembre, n. 229 • ISSN 2035-5866
DOI 10.23827/BDL_2020_3_4
Nuova serie [www.centroeinaudi.it]

Da qui la necessità di esplorare vie non convenzionali di assistenza e cura, prevedendo anche l'utilizzo di nuovi strumenti tecnologici, come ad esempio gli *assistive robots* (Birnbaum *et al.* 1984; Mihailidis *et al.* 2001; Coughlin *et al.* 2006; Bennet, Hauser 2013; Tao, McRoy 2015; Okamura, Mataric, Christensen 2010; Shibata, Wada 2010; Bemelmans *et al.* 2012; Eriksson, Salzmann-Erikson 2017).

Ciò ha portato a sviluppare diverse riflessioni in ambito filosofico e bioetico in termini di autonomia dell'anziano nel contesto delle cure ove si deve operare un bilanciamento tra istanze di promozione della stessa (*active aging*) e atteggiamenti di protezione (Sanchini, Sala 2019) senza dimenticare una possibile modifica degli standard morali, che ci vedrebbe favorevoli ad accettare situazioni in cui l'anziano si trovi a essere potenzialmente ancora più isolato e in un legame affettivo *one-sided* (Sparrow, Sparrow 2006; Borenstein, Pearson 2010; Sharkey, Sharkey 2010a, 2010b; Coeckelbergh 2010, 2015; De Graaf 2016).

Ma accanto a queste corrette considerazioni, riteniamo che ve ne siano altre di tipo criminologico relative ai possibili rischi associati all'uso non etico se non illegale di queste tecnologie, che, come vedremo, hanno *in re ipsa* una loro vulnerabilità che può trasformarsi in opportunità criminale.

Per meglio chiarire questa ultima frase che potrebbe sembrare criptica è necessario svolgere una riflessione su caratteristiche e funzioni di questi dispositivi.

2. *Assistive robot*, tra tecnologia e rischi

Gli *assistive robot* sono progettati e costruiti per fornire aiuto o supporto a chi li utilizza. In letteratura si distinguono in *rehabilitation robot*, creati per essere un supporto fisico; e *social robot*, macchine pensate per una possibile interazione con l'utilizzatore, dotate di capacità motorie e/o manipolative e di un'interfaccia che racchiude tutte le caratteristiche che permettono di attribuire al dispositivo, appunto, qualità sociali (Kachoui *et al.* 2014; Robinson *et al.* 2014; Abdi *et al.* 2018). Un'ulteriore distinzione è tra *service robots*, realizzati per supportare le persone nei compiti di vita quotidiana e nella mobilità, monitorandone al contempo salute e sicurezza; e *companion robots*, il cui scopo è "inserirsi" nella vita delle persone come una sorta di compagno virtuale (Kachoui *et al.* 2014; Robinson *et al.* 2014; Abdi *et al.* 2018; Feil-Seifer, Mataric 2005, 2009, 2011). Si tratta di macchine com-

plesse, dotate di intelligenza artificiale (IA) che le rende in grado di processare e analizzare in brevissimo tempo un'enorme quantità di dati oltre che di imitare i processi cognitivi del cervello umano. Invero, i software di intelligenza artificiale, elaborando gli stimoli che provengono dall'interlocutore, permettono loro di fornire risposte adeguate, favorendo così la relazione.

Inoltre, sono progettati con un design umano al fine di agevolare l'interazione degli utenti con i dispositivi, sfruttando la tendenza tipicamente umana all'antropomorfismo (Timpano, Shaw 2013; Scheele *et al.* 2015; Epley, Waytz, Cacioppo 2007). Infatti, il corpo meccanico dei SARs è progettato per richiamare le sembianze umane ed è dotato non solo di componenti visive e sonore, come occhi e bocca, attraverso cui vengono raccolti stimoli e informazioni da e sull'utente, ma anche di abilità motorie, circoscritte alla mimica facciale (espressa attraverso i movimenti di sopracciglia o degli altri elementi del viso) o estese a tutto il corpo in base al tipo di robot (Allwood 2002; Fong *et al.* 2003; Zani *et al.* 2003; Tapus, Mataric, Scassellatti 2007). Attraverso queste dotazioni e con il supporto dei sistemi di IA il dispositivo può sfruttare le varie opzioni sensoriali per coinvolgere socialmente la persona e, allo stesso tempo, può perseguire lo scopo di fornire supporto nei compiti quotidiani, in comportamenti pro-sociali e nelle questioni di salute (Scoglio *et al.* 2019).

In aggiunta va rilevato che tali dispositivi possono raccogliere, interpretare e apprendere dai dati acquisiti attraverso processi di *machine learning* e *decision making* che, esattamente come nel caso dell'apprendimento umano, si basano su metodi di *trial and error* (Mihailidis *et al.* 2001; Bennet, Hauser 2013). Per incrementare la potenza di calcolo e lo spazio di archiviazione delle informazioni, questi robot possono inoltre essere parte del così detto *cloud* o nuvola informatica, ovvero un apparato che, attraverso l'uso della rete Internet, crea un ecosistema di condivisione complesso, inseparabile e ad alta velocità tra i dispositivi associati e i meccanismi di calcolo e di raccolta informazioni collocati in remoto nella nuvola informatica (Fosch-Villaronga, Albo-Canals 2019). Questa tipologia di struttura li rende in grado da un lato di avere una connessione efficiente e costante con familiari e operatori sanitari, e dall'altro di monitorare e rilevare continuamente informazioni utili sul soggetto.

Come si diceva, gli *assistive robots* possono assumere diversi ruoli nell'ambito dell'assistenza all'anziano: quello di promemoria, ad esempio per visite o appuntamenti; di training cognitivo e/o affettivo, potenziando le funzioni cognitive e migliorando l'umore e il benessere dell'individuo; di coaching,

assistendo negli esercizi di riabilitazione; di facilitatore sociale e/o compagno, fungendo da mezzo per favorire la socializzazione e per ridurre il senso di solitudine e isolamento; e non da ultimo di monitor dello stato di salute e canale comunicativo con i *caregiver* (Fong *et al.* 2002; Pineau *et al.* 2003; Wada *et al.* 2004; Kyong *et al.* 2005; Tapus, Tapus, Mataric 2009; Sharkey, Sharkey 2010a; Fasola, Mataric 2013; McGlynn *et al.* 2014; Rabbitt *et al.* 2015; van Kemenade *et al.* 2015; Abdi *et al.* 2018).

In questo contesto di emergenza sanitaria connessa alla diffusione pandemica legata al Covid-19, l'utilità e l'utilizzo di questi dispositivi robotici è cresciuta[2]. Un robot non rischia né di infettarsi né di trasmettere la malattia ma può acquisire informazioni fondamentali relativamente a un paziente ancora in grado di interagire. Si tratta di concrete opportunità di utilizzo che come detto poc'anzi non sono esenti da rischi anche di tipo criminale. Queste macchine possono essere trasformate in formidabili "grimaldelli virtuali" in grado di rubare informazioni preziose e riservate sulla vita anche economica delle persone che le utilizzano.

Non dobbiamo mai dimenticare come il crimine sia una sorta di camaleonte in grado di adattarsi perfettamente ai cambiamenti sociali (Travaini, Caruso, Merzagora 2020), e che possa trovare in questo mutamento nell'*aging care* un possibile vantaggio.

3. L'acquisizione o la divulgazione di informazioni

Occorre partire da un semplice dato; un *socially assistive robot*, così come qualunque altro dispositivo connesso alla rete, può essere *hackerato* per scopi criminali (Jones 2018; Apa, Cerrudo 2017; Hatfield 2018; King *et al.* 2018).

[2] Riportiamo di seguito la trascrizione delle parti di intervista del Professor Guang-Zhong Yang, preside dell'istituto di Robotica Medica presso l'Università Jiao Tong di Shangai, a cui ci siamo riferiti: «Robots can be really useful to help you manage this kind of situation, whether to minimize human-to-human contact or as a front-line tool you can use to help contain the outbreak». Successivamente lo studioso afferma: «You probably saw that Italy has imposed a total lockdown. That could have a major psychological impact, particularly for people who are vulnerable and living alone. There is one area of robotics, called social robotics, that could play a part in this as well». La versione integrale dell'intervista è disponibile al seguente indirizzo:https://spectrum.ieee.org/automaton/robotics/medical-robots/coronavirus-pandemic-call-to-action-robotics-community.

Sono macchine autonome in grado di comunicare e interagire con le persone, possono raccogliere, archiviare e trasmettere in tempo reale enormi quantità di dati sull'utente e sull'ambiente circostante. Ed è proprio la connessione *cloud* la maggior vulnerabilità di questi dispositivi (Rodríguez *et al.* 2017; Bathaee 2018)[3].

Il rischio è una condivisione, non voluta o forzata, di dati sicuramente sensibili con una significativa violazione della privacy dell'utente e nelle quattro dimensioni di *physical, psychological, social* e *information privacy* (Lutz, Scöttler, Hoffmann 2019).

Il quadro così rappresentato ci porta a immaginare la presenza di diversi attori con diversi ruoli. Da un lato una persona anziana che ha buone possibilità di diventare una vittima, e dall'altro criminali informatici abili, super tecnologici e caratterizzati in moltissimi casi da totale assenza di empatia rispetto alla vittima, pur se fragile e molte volte indifesa.

L'*assistive robot* con cui si era creato un rapporto di fiducia, divenuto parte della propria casa e della propria vita può diventare, nelle mani sbagliate, l'oggetto che ci "colpisce" e "tradisce".

Tutti le informazioni ottenute possono permettere in concreto di sottrarre denaro dai conti corrente, così come favorire l'ingresso nell'abitazione per sottrarre beni di valore o creare, con le informazioni sensibili, una identità virtuale utilizzata per traffici illegali. La vittima si troverà così intestataria di autovetture utilizzate per furti e rapine se non destinataria di materiale di ogni genere, sovente illegale. Il tutto è antigiuridico in quanto va a violare norme codificate dal nostro Codice penale. Inoltre, le medesime condotte potrebbero essere aggravate ai sensi dell'art. 61 comma 5 del

[3] Nel loro articolo, Rodríguez *et al.* (2017) distinguono i modi in cui il funzionamento di un robot può essere intaccato. In primo luogo, un robot può cambiare il normale modo di operare a livello pratico («in a physical way»). Questo cambiamento può essere dovuto a una condizione naturale, a una situazione accidentale ma anche a un attacco informatico, e le conseguenze possono essere: distruzione, che comporta la non operatività del dispositivo; danno parziale, che porta al malfunzionamento del robot; interruzione di una o più componenti del robot; degradazione delle capacità del dispositivo dovuta allo scorrere del tempo; e infine comportamento inatteso, che può essere considerato come un peggioramento dell'intero robot e non solo di un suo componente. In secondo luogo, il funzionamento del robot può essere condizionato a livello virtuale («in a virtual way»), il che vuol dire che può essere modificato il modo in cui le informazioni sono raccolte, immagazzinate e trasmesse dal robot.

Codice penale che considera condizione di vulnerabilità l'età della possibile vittima.

In letteratura criminologica si è cercato di comprendere i meccanismi psicologici che permettono agli autori di questi crimini di commettere e giustificare tali condotte (Lickiewicz 2011; Wada, Longe, Danquah 2012; Sabillon *et al*. 2016).

È ben noto, come evidenziato per primi da Sykes e Matza (1957), che in capo a chi commette un reato, operino delle tecniche chiamate di neutralizzazione che riducendo le dissonanze cognitive derivanti dalla condotta criminale, permettono di attenuare o ridurre l'attribuzione di colpa. L'azione pur criminosa viene mitigata da motivazioni che rendono il proprio agire tollerabile se non giustamente motivato. Più queste giustificazioni morali sono presenti e meno potrà attivarsi in capo all'autore quel processo di consapevolezza del disvalore giuridico e morale del gesto che è alla base di una riduzione di una possibile recidiva. In estrema sintesi, più si è in grado di giustificare la propria condotta e più cresce il rischio che si continui a delinquere. Vi sono alcune tecniche di neutralizzazione che più di altre si adattano al criminale informatico; ci riferiamo alla negazione della vittima e alla minimizzazione del danno. Occorre pensare come si operi una sorta di distinzione tra ciò che è male nel mondo fisico e ciò che è male nel mondo virtuale, reputando come di minor entità i danni arrecanti in quest'ultimo in quanto non tangibili. Appare più semplice recare danno ad altri quando il loro dolore non è visibile e quando comportamenti dannosi sono fisicamente e temporalmente lontani dai loro effetti nocivi (Bandura 2002). In questo tipo di crimini la distanza fisica dalla persona che subisce l'attacco facilita anche la distanza emotiva.

Suler (2004) individua diversi elementi che nel mondo virtuale portano le persone ad assumere un atteggiamento più disinibito rispetto a quello che avrebbero nel mondo reale. Secondo l'autore sono almeno sei i fattori che facilitano la commissione di crimine attraverso la rete oltre alle predisposizioni individuali di ognuno: anonimità dissociativa (*dissociative anonimity*); invisibilità (*invisibility*); asincronia (*asynchronicity*); introiezione solipsistica (*solipsistic introjection*); immaginazione dissociativa (*dissociative immagination*) e minimizzazione dello status e dell'autorità (*minimization of status and authority*). Come il meccanismo della negazione della responsabilità di Sykes e Matza, anche l'anonimità dissociativa (*dissociative anonimity*) permette di incidere sulla consapevolezza dell'individuo, il quale smette di considerarsi come l'agente reale delle sue stesse azioni. Il "sé online" si costituisce come

quella parte dell'identità della persona stanziata sul web e a cui è reso possibile evitare l'attribuzione di responsabilità per i propri comportamenti, quasi come se le restrizioni e i processi mentali legati alla morale per questa istanza del sé venissero temporaneamente sospesi. A ciò deve essere aggiunta la facoltà di risultare invisibili navigando sul web (*invisibility*), il che è permesso da un lato dalla modalità di comunicazione solo testuale, dall'altro dalla possibilità di navigare online in forma anonima. Elemento questo che, insieme all'asincronismo delle risposte (*asynchronicity*) permette di evitare di dover gestire reazioni immediate e magari avverse, limitando la percezione del disagio creato.

Suler spiega inoltre la possibilità di dissociarsi facilmente da ciò che succede online creando un personaggio immaginario (*dissociative immagination*). Questo è reso possibile dall'introiezione della realtà virtuale (*solipsistic introjection*) nell'immaginazione della persona. La creazione di un personaggio immaginario, rileva l'autore, non è qualcosa di inconsueto, anzi, le persone utilizzano spesso questo meccanismo immaginativo per figurarsi esiti diversi di avvenimenti e conversazioni, o per ipotizzare nuovi scenari. Questa convergenza di fattori potrebbe facilitare la generazione di credenze che vanno a inibire i meccanismi di controllo morale. Se a questo processo vengono poi a sommarsi la mancanza di un controllo centralizzato del mondo virtuale (*minimization of status and authority*) e la possibilità di abbandonare o distaccarsi da ciò che avviene si ottiene un effetto disinibitorio amplificato che può portare la persona a sperimentare una separazione tra *mens rea* e *actus reus*, ovvero a percepire il sé online come distinto e divincolato da tutto ciò che riguarda il mondo reale scaturendo di fatto nella disinibizione dei comportamenti alla base di condotte criminali.

Anche secondo Karuppannan Jaishankar (2008), l'anonimato fornito dal mondo virtuale facilita una sorta di de-individualizzazione, sottolineando che l'effetto è simile all'indossare una maschera dietro alla quale nessuno può identificare l'identità reale della persona. Una maschera favorita dal fatto che nella criminalità informatica vi è un minor rischio di essere individuati e, cosa di non poco conto, sono limitati i processi di stigmatizzazione collettiva di fronte a questo tipo di criminale, talvolta considerato prima geniale e poi delinquente.

In aggiunta, come osservato da diversi autori (Becker 1968; Cornish, Clarke 1987), nel comportamento criminale è possibile rinvenire una componente razionale di calcolo che riguarda vantaggi e svantaggi derivanti

dall'azione. Chi delinque, nel ponderare l'attuabilità del crimine, valuterà da un lato i benefici ricavabili dal compimento dell'atto reo e dall'altro i costi, diretti e indiretti, a cui esporrebbe una scelta di questo tipo. La riduzione delle utilità attese dal compimento dell'azione criminale, siano esse economiche o il piacere derivante dal soddisfacimento di pulsioni, è determinata dal mutare di due valori: la probabilità che il crimine venga scoperto e la relativa pena. Per contro, l'incremento dei costi è dato non solo dallo sforzo richiesto da organizzazione ed esecuzione del reato (costi diretti), ma anche da ipotizzabili contrasti interni, violazioni dei valori etici e sociali ed eventuali compromissioni di legami affettivi significativi per il soggetto (costi indiretti). Tutti questi fattori confluiscono nella valutazione della commissione del fatto illecito e, se i benefici attesi superano rischi e costi, allora l'individuo si determinerà a delinquere.

Nel caso di un criminale informatico che decidesse di sfruttare un robot addetto alla cura di un anziano, si realizzerebbe una "felice" convergenza di fattori; bassi costi diretti riguardanti l'elaborazione della linea di codice che alteri il funzionamento del robot e di pianificazione del modo opportuno di agganciarsi al dispositivo per lanciare l'attacco. Da sommare al fatto che la vittima, non accorgendosi dell'attacco subito, facilmente non presenterà denuncia alle autorità competenti. A tutto ciò va aggiunto una normativa di non facile applicazione che porta ad avere a livello internazionale bassi tassi di incriminazione per questo tipo di reati informatici (Young, Zhang, Prybutok 2007; Eoyang *et al.* 2018; Kranenbarg *et al.* 2018; IC3 Report 2019). In altre parole, si tratta di un nuovo fattore di rischio accanto a quelli più tradizionali, ovvero persone che invece di dedicarsi alla cura del soggetto anziano cercano di trarne un vantaggio di tipo economico con comportamenti che vanno solitamente a configurare i reati di appropriazione indebita, furto, sostituzione di persona e nei casi più gravi la circonvenzione di incapace. Anche per questa tipologia di reati vi è un altissimo numero oscuro che limita l'aver un quadro oggettivo del fenomeno (Jackson, Hafemeister 2011; Mysyuk, Westendorp, Lindenberg 2016; Pillemer *et al*. 2016; Santos *et al.* 2019).

L'insieme di queste valutazioni porta a immaginare come questo tipo di condotta non potrà che crescere nel futuro in maniera significativa. Ma cosa è possibile fare per bilanciare sviluppo di queste tecnologie e protezione per chi le utilizza?

4. Un quadro di sintesi

È opportuno considerare che si è di fronte a un crimine estremamente recente per cui non vi è ancora una normativa *ad hoc* e le stesse agenzie di *law enforcement* stanno sviluppando programmi di contrasto definiti. In altre parole, le caratteristiche evolutive del fenomeno limitano valutazioni che non siano descrittive dello stato dell'arte del fenomeno. Esistono, però, delle strategie di prevenzione che crediamo valga la pena condividere.

In primis, chi utilizza questi *assistive robots* dovrebbe essere ben informato non solo su funzioni e capacità del prodotto, ma anche sui possibili rischi criminali connessi all'uso. Un'informazione mirata, comprensibile e il più incoraggiante possibile. Un'attività formativa adeguata a tipologia ed età degli utenti, magari proveniente da canali istituzionali. In questo senso è lodevole l'attività di informazione volta alla popolazione italiana da parte della polizia postale per i reati di truffa informatica. È importante il riconosciuto valore dell'ente formatore in quanto permette di superare la fisiologica diffidenza che può caratterizzare la non giovane età.

La letteratura ci insegna come la formazione sia il più utile strumento di prevenzione per limitare il più possibile i tentativi di attacchi informatici (Chantler, Broadhurst 2006; Luo *et al.* 2011; Gragg 2003; King *et al.* 2018; Montañez, Golob, Xu 2020). Tale attività dovrebbe coinvolgere l'anziano allor quando in grado di comprenderla ma soprattutto coloro che se ne occupano. Pertanto, diventa ancora più importante la costruzione e il consolidamento di una rete sociale atta ad accogliere e a rispondere ai bisogni dell'individuo, ma anche con una maggiore conoscenza dei possibili rischi. Una formazione che dovrà essere continua in quanto, come più volte indicato, il crimine informatico si caratterizza per una evoluzione velocissima. Ciò che probabilmente stiamo dicendo ora potrebbe essere superato da nuove condotte criminali.

Da ultimo, non bisogna dimenticare gli effetti estremamente negativi che una qualsiasi azione criminale può avere su un soggetto anziano. Ogni vittima del crimine "paga un prezzo" elevato in termini fisici, economici ma soprattutto psichici, prezzo che cresce in maniera significativa in caso di fragilità fisica ed emotiva ove l'azione criminale può trasformarsi in un vero e proprio trauma talvolta non facile da superare. Nel caso di un uso illegale del proprio *social robot*, l'anziano potrebbe sperimentare una grave sensazione di tradimento nei confronti del dispositivo verso cui aveva sviluppato sentimen-

ti di fiducia e affezione. Questo danno psicologico, totalmente ignorato dal criminale, ha invece pari rilevanza e influenza di quello economico nella vita delle vittime di questi crimini (Button, Lewis, Tapley 2014; Yunus, Hairi, Yuen 2017; Zhang *et al.* 2018).

Siamo dunque di fronte a nuove opportunità tecnologiche sulle quali è necessario svolgere considerazioni filosofiche e bioetiche ma che, considerati i rischi connessi, necessitano parimenti di riflessioni criminologiche. La soluzione proposta è quella di una maggiore consapevolezza, di una informazione e formazione costante nonché di una divulgazione dei danni provocati. Su questo ultimo punto occorrerà immaginare una particolare attenzione comunicativa al fine di evitare che l'aspetto del rischio possa diventare prevalente rispetto all'eventuale utilità della macchina.

In estrema sintesi, di fronte a un fenomeno in così rapida evoluzione siamo consapevoli di aver semplicemente svolto una descrizione dello stesso. Come accade, però, in ambito criminologico l'aver evidenziato e condiviso i possibili rischi crediamo possa da un lato, aumentare la consapevolezza delle vittime, e dall'altro favorire la stigmatizzazione degli autori.

Bibliografia

Abdi J., Al-Hindawi A., Ng T., Vizcaychipi M. (2018), "Scoping Review on the Use of Socially Assistive Robot Technology in Elderly Care", *BMJ Open*, n. 8, e018815.

Allwood J. (2002), "Bodily Communication Dimensions of Expression and Content", in B. Granström *et al.* (a cura di), *Multimodality in Language and Speech Systems*, Boston, Kluwer Academic, pp. 7-26.

Apa L., Cerrudo C. (2017), "Hacking Robots Before Skynet", Seattle, IOActive Inc., pp. 1-17, https://ioactive.com/pdfs/Hacking-Robots-Before-Skynet.pdf.

Arslantaş H., Adana F., Abacigil Ergin F., Kayar D., Acar G. (2015), "Loneliness in Elderly People, Associated Factors and Its Correlation with Quality of Life: A Field Study from Western Turkey", *Iran J Public Health*, vol. 44, n. 1, pp.43-50.

Bandura A. (2002), "Selective Moral Disengagement in the Exercise of Moral Agency", *Journal of Moral Education*, vol. 31, n. 2, pp. 101-119.

Bathaee Y. (2018), "The Artificial Intelligence Black Box And The Failure Of Intent And Causation", *Harvard Journal of Law & Technology*, vol. 31, n. 2, pp. 889-938.

Becker G.S. (1968), "Crime and Punishment: An Economic Approach", *Journal of Political Economy*, n. 76, pp. 169-217.

Bemelmans R., Gelderblom G., Jonker P., de Witte L. (2012), "Socially Assistive Robots in Elderly Care: A Systematic Review into Effects and Effectiveness", *Journal of American Medical Directors Association*, vol. 13, n. 2, pp. 114-120.

Bennet C., Hauser K. (2013), "Artificial Intelligent Framework for Simulating Clinical Decision- Making: A Markov Decision Process Approach", *Artificial Intelligence in Medicine*, vol. 57, n.1, pp. 9-19.

Birnbaum H., Burke R., Sweringen C., Dunlop B. (1984), "Implementing Community Based Long-term Care: Experience of New York's Long-term Home Health Care Program", *The Gerontologist*, n. 24, pp. 380-386.

Borenstein J., Pearson Y. (2010), "Robot Caregivers: Harbingers of Expanded Freedom for All?", Et*hics of Information Technology*, vol. 12, pp. 277-288.

Button M., Lewis C., Tapley J. (2014), "Not a Victimless Crime: The Impact of Fraud on Individual Victims and their Families", *Security Journal*, vol. 7, n. 1, pp. 36-54.

Chantler A., Broadhurst R. (2006), "Social Engineering and Crime Prevention in Cyberspace" - Technical Report, Brisbane, Queensland University of Technology.

Coeckelbergh M. (2015), "Artificial Agents, Good Care, and Modernity", *Theoretical Medicine and Bioethics*, vol. 36, pp. 265-277.

– (2010), "Health Care, Capabilities, and AI Assistive Technologies", *Ethic Theory Moral Practice*, n. 13, pp. 181-190.

Congzhi H., Jingzhong Y. (2014), "Lonely Sunsets: Impacts of Rural-urban Migration on the Left-behind Elderly in Rural China", *Population, Space and Place*, Special Issue: *Rural Migration, Agrarian Change and Institutional Dynamics: Perspectives from the Majority World*, vol. 20, n. 4, pp. 352-369.

Cornish D.B., Clarke B.V. (1987), "Understanding Crime Displacement: An Application Of Rational Choice Theory", *Criminology*, vol. 25, n. 4, pp. 933-948.

Coughlin J., Pope E., Leedle B. (2006), "Old Age, New Technology, and Future Innovations in Disease Management and Home Health Care", *Home Health Care Management & Practice*, vol. 18, n. 3, pp. 196-207.

De Graaf M. (2016), "An Ethical Evaluation of Human-Robot Relationship", *International Journal of Social Robotics*, vol. 8, pp. 589-598.

Dury R. (2014), "Social Isolation and Loneliness in the Elderly: An Exploration of Some of the Issues", *British Journal of Community Nursing*, vol. 19, n. 3, pp. 125-128.

Eoyang M., Peters A., Mehta I., Gaskew B. (2018), "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors", *Third Way*, 29 ottobre 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors.

Epley N., Waytz A., Cacioppo J.T. (2007), "On Seeing Human: A Three-factor Theory of Anthropomorphism", *Psychological Review*, vol. 114, n. 4, pp. 864-886.

Eriksson H., Salzmann-Erikson M. (2017), "The Digital Generation and Nursing Robotics: A Netnographic Study about Nursing Care Robots Posted on Social Media", *Nursing Inquiry*, n. 24, e12165.

Fasola J., Mataric M. (2013), "A Socially Assistive Robot Exercise Coach for the Elderly", *J Hum Robot Interact*, vol. 2, n. 2, DOI: 10.5898/jhri.2.2.fasola.

Feil-Seifer D., Mataric M. (2011), "Ethical Principles for Socially Assistive Robotics", *IEEE Robotics & Automation Magazine*, vol. 18, n. 1, pp. 24-31.

– (2009), "Human-Robot Interaction", in *Encyclopedia of Complexity and Systems Science*, pp. 4643-4659, DOI: 10.1007/978-0387-30440-3_274.

– (2005), "Defining Socially Assistive Robotics", Proceedings of the 2005 IEEE 9th International Conference on Rehabilitation Robotics, Chicago.

Fong T., Nourbakhsh I., Dautenhahn K. (2003), "A Survey of Socially Interactive Robots", *Robotics and Autonomous System*, vol. 42, pp. 143-166.

– (2002), "A Survey of Socially Interactive Robots: Concepts, Design, and Applications", Tech. Report, CMU-RI-TR-02-29, Robotics Institute, Carnegie Mellon University.

Fosch-Villaronga E., Albo-Canals J. (2019), "I'll Take Care of You, Said the Robot", *Paladyn, Journal of Behavioral Robotics*, vol. 10, n. 1, pp. 77-93, DOI: https://doi.org/10.1515/pjbr-2019-0006.

Freedman W.A. (1996), "Family Structure and Risk of Nursing Home Admission", *J Gerontol*, vol. 2, pp. 61-69.

Fujisawa R., Colombo F. (2009), "The Long-term Care Workforce: Overview and Strategies to Adapt Supply to a Growing Demand", OECD Health Working Papers, n. 44, OECD Publishing.

Golden J., Conroy R.M., Bruce I., Denihan A., Greene E., Kirby M., Lawlor B.A. (2009), "Loneliness, Social Support Networks, Mood and Wellbeing in Community-dwelling Elderly", *International Journal of Geriatric Psychiatry*, vol. 24, n. 7, pp. 694-700.

Gragg D. (2003), *A Multi-level Defense Against Social Engineering*, SANS Institute Information Security Reading Room.

Grinin L., Korotayev A. (2016), "Global Population Ageing, the Sixth Kondratieff Wave, and the Global Financial System", *Journal of Globalization Studies*, vol. 7, n. 2, pp. 11-31.

Haddad L.M. (2019), *Nursing Shortage*, National Center for Biotechnology Information, https://www.ncbi.nlm.nih.gov/books/NBK493175/.

Hatfield J.M. (2018), "Social Engineering in Cybersecurity: The Evolution of a Concept", *Computer & Security*, vol. 73, pp. 102-113.

Internet Crime Complaint Center (IC3), FBI, *Internet Crime Report* (2019), https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120.

Jackson S., Hafemeister T. (2011), "Risk Factors Associated with Elder Abuse: The Importance of Differentiating by Type of Elder Maltreatment", *Violence and Victims*, vol. 26, n. 6, pp. 738-757.

Jaishankar K. (2008), "Space Transition Theory of Cybercrimes", in F. Schmallager, M. Pittaro (a cura di), *Crimes of the Internet*, Upper Saddle River (NJ), Prentice Hall, pp. 283-301.

Jones R. (2018), "Engineering Cheerful Robots: An Ethical Consideration", *Information*, vol. 9, n. 7, pp. 152-163.

Kachouie R., Sedighadeli S., Khosla R., Chu M. (2014), "Socially Assistive Robots in Elderly Care: A Mixed-method Systematic Literature Review", *International Journal of Human-Computer Interaction*, vol. 30, pp. 369-393.

King T.C., Aggarwal N., Taddeo M., Floridi L. (2018), "Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions", *Science and Engineering Ethics*, https://doi.org/10.1007/s11948-018-00081-0.

Kranenbarg M.W., Ruiter S., van Gelder J.L., Bernasco W. (2018), "Cyber-Offending and Traditional Offending over the Life-Course: An Empirical Comparison", *J Dev Life Course Criminology*, vol. 4, pp. 343-364.

Kyong I.K., Freedman S., Mataric M., Cunningham M., Lopez B. (2005), "A Hands-off Physical Therapy Assistance Robot for Cardiac Patients", presented at 9th International Conference on Rehabilitation Robotics, Chicago.

Landeiro F., Barrows P., Nuttall Musson E., Gray A., Leal J. (2017), "Reducing Social Isolation and Loneliness in Older People: A Systematic Review Protocol", *BMJ Open*, vol. 7, n. 5.

Lickiewicz J. (2011), "Cyber Crime Psychology – Proposal Of An Offender Psychological Profile", *Problems of Forensic Sciences*, vol. LXXXVII, pp. 239-252.

Liu J.X., Goryakin Y., Maeda A., Bruckner T., Scheffler R. (2017), "Global Health Workforce Labor Market Projections for 2030", *Human Resources for Health*, vol. 15, n. 11, DOI: 10.1186/s12960-017-0187-2.

Luo X., Brody R., Seazzu A., Burd S. (2011), "Social Engineering: The Neglected Human Factor Information Security Management", *Information Resources Management Journal*, vol. 24, n. 3, pp. 1-8.

Lutz C., Scöttler M., Hoffmann C. (2019), "The Privacy Implication of Social Robots: Scoping Review and Expert Interviews", *Mobile, Media & Comunication*, vol. 7, n. 3, pp. 412-434.

McGlynn S., Snook B., Kemple S., Mitzner T., Rogers W. (2014), "Therapeutic Robots for Older Adults: Investigating the Potential of Paro", Proceedings of the 2014 ACM/IEEE International Conference on Human-robot Interaction, pp. 246-247, New York.

Mihailidis A., Fernie G., Barbenel J. (2001), "The Use of Artificial Intelligence in the Design of an Intelligent Cognitive Orthosis for People with Dementia", *Assistive Technology*, vol. 13, n. 1, pp. 23-39.

Montañez R., Golob E., Xu S. (2020), "Human Cognition Through the Lens of Social Engineering Cyberattacks", *Frontiers in psychology*, vol. 11, n. 1755, pp. 1-18.

Murray M. (2002), "The Nursing Shortage: Past, Present, and Future", J*ONA: The Journal of Nursing Administration*, vol. 32, n. 2, pp. 79-84.

Mysyuk Y., Westendorp R.G.J., Lindenberg J. (2016), "How Older Persons Explain Why They Became Victims of Abuse", *Age and Ageing*, vol. 45, n. 5, pp. 695-702.

OECD (2019), *Health at a Glance 2019: OECD Indicators*, Paris, OECD Publishing, https://doi.org/10.1787/4dd50c09-en.

Okamura A., Mataric M., Christensen H. (2010), "Medical and Health-Care Robotics", *IEEE Robotics & Automation Magazine*, vol. 17, n. 3, pp. 26-37.

Pearce D., Cantisani G., Laihonen A. (1999), "Changes in Fertility and Family Sizes in Europe", *Population Trends*, n. 95, pp. 33-40.

Pillemer K., Burnes D., Riffin C., Lachs M. (2016), "Elder Abuse: Global Situation, Risk Factors, and Prevention Strategies", *The Gerontologist*, vol. 56, n. S2, pp. 194-205.

Pineau J., Montemerloa M., Pollackb M., Roy N., Thrun S. (2003), "Towards Robotic Assistants in Nursing Homes: Challenges and Results", Special *Issue on Socially Interactive Robots, Robotics and Autonomous Systems*, vol. 1048, pp. 1-11.

Rabbitt S.M., Kazdin A.E., Scassellati B. (2015), "Integrating Socially Assistive Robotics into Mental Healthcare Interventions: Applications and Recommendations for Expanded Use", *Clinical Psychology Review*, vol. 35, pp. 35-46, DOI: 10.1016/j.cpr.2014.07.001.

Robinson H., MacDonald B., Broadbent E. (2014), "The Role of Healthcare Robots for Older People at Home: a Review", *International Journal of Social Robotics*, vol. 6, pp. 575-591.

Rodríguez F.J., Fernández C., Guerrero A.M., Matellán Olivera V. (2017), "Cybersecurity of Robotics and Autonomous Systems: Privacy and Safety", *Robotics - Legal, Ethical and Socioeconomic Impacts*, pp. 75-90, http://dx.doi.org/10.5772/intechopen.69796.

Sabillon R., Cano J., Cavaller V., Serra J. (20106), "Cybercrime and Cybercriminals: A Comprehensive Study", *International Journal of Computer Networks and Communications Security*, vol. 4, n. 6, pp. 165-176.

Sanchini V., Sala R. (2019), "Oltre la protezione che rende soli. Coltivare l'autonomia dell'anziano nel contesto delle cure", *NEU Rivista di Formazione Infermieristica*, n. 3, pp. 6-14.

Sands L., Wang Y., McCabe G., Jennings K., Eng C., Covinsky K. (2006), "Rates of Acute Care Admissions for Frail Older People Living with Met Versus Unmet Activity of Daily Living Needs", *JAM Geriatr. Soc*, vol. 54, pp. 339-344.

Santos A.J., Nunes B, Kislaya I., Gil A.P., Ribeiro O. (2019), "Older Adult's Emotional Reactions to Elder Abuse: Individual and Victimisation Determinants", *Health and Social Care in the Community*, vol. 27, n. 3, pp. 609-620.

Scheele D., Schwering C., Elison J., Spunt R., Maier W., Hurlemann R. (2015), "A Human Tendency to Anthropomorphize is Enhanced by Oxytocin", *European Neuropsychopharmacology*, vol. 25, n. 10, pp. 1817-1823.

Scheffler R., Cometto G., Tulenko K. (2016), "Health Workforce Requirements for Universal Health Coverage and the Sustainable Development Goals", background paper n. 1 to the WHO Global Strategy on Human Resources for Health: Workforce 2030, Geneva, World Health Organization, http://www.who.int/hrh/resources/health-observer17/en/.

Scheutz M. (2009), "The Inherent Dangers of Unidirectional Emotional Bonds between Humans and Social Robots", Conference paper: Workshop on Roboethics at ICRA.

Scoglio A., Reilly E.D., Gorman J.A., Drebing C.E. (2019), "Use of Social Robots in Mental Health and Well-Being Research: Systematic Review", *Journal of Medical Internet Research*, vol. 21, n. 7, e13322, DOI: 10.2196/13322.

Sharkey A., Sharkey N. (2010a), "Granny and the Robots: Ethical Issues in Robot Care for the Elderly", *Ethics Inform. Technol.*, n. 14, pp. 27-40, DOI: 10.1007/s10676010-9234-6.

– (2010b), "The Crying Shame of Robot Nannies: An Ethical Appraisal", *Interaction Studies*, vol. 11, n. 2, DOI: 10.1075/is.11.2.01sha.

Shibata T., Wada K. (2010), "Robot Therapy: A New Approach for Mental Healthcare of the Elderly-a Mini-review", *Gerontology*, vol. 57, pp. 378-386, DOI: 10.1159/000319015.

Shu-Chuan J.Y., Sing Kai L. (2004), "Living Alone, Social Support, and Feeling Lonely among the Elderly", *Social Behavior and Personality: an international journal*, vol. 32, n. 2, pp. 129-138.

Sparrow R., Sparrow, L. (2006), "In the Hands of Machines? The Future of Aged Care", *Minds Machines*, vol. 16, pp. 141-161, DOI: 10.1007/s11023-006-9030-6.

Suler J. (2004), "The Online Disinhibition Effect", *Cyberpsychology & Behavior*, vol. 7, n. 3, pp. 321-326.

Sykes G.M., Matza D. (1957), "Techniques of Neutralization: A Theory of Delinquency", *American Sociological Review*, vol. 22, n. 6, pp. 664-670.

Tao H., McRoy S. (2015), "Caring for and Keeping the Elderly in Their Homes", *Chinese Nursing Research*, vol. 2, nn. 2-3, pp. 31-34.

Tapus A., Mataric M., Scassellatti B. (2007), "The Grand Challenges in Socially Assistive Robotics", *IEEE Robotics and Automation Magazine*, vol. 14, n. 1, pp. 35-42.

Tapus A., Tapus C., Mataric M. (2009), "The Use of Socially Assistive Robots in the Design of Intelligent Cognitive Therapies for People with Dementia", Proceedings of the International Conference on Rehabilitation Robotics, pp. 924-929.

Timpano K., Shaw A.M. (2013), "Conferring Humanness: The Role of Anthropomorphism in Hoarding", *Personality and Individual Differences*, vol 54, n. 3, pp. 383-388, DOI: 10.1016/j.paid.2012.10.007.

Travaini G., Caruso P., Merzagora I. (2020), "Crime in Italy at the Time of the Pandemic", *Acta Biomed*, vol. 91, n. 2, DOI: 10.23750/abm.v91i2.9596.

United Nations Office On Drugs And Crime Vienna (2013), "Comprehensive Study on Cybercrime", Draft, United Nations, New York.

United Nations, Department of Economic and Social Affairs, Population Division (2019), *World Population Prospects 2019*, vol. II: *Demographic Profiles*.

Van Kemenade M., Konijn E., Hoorn J. (2015), "Robots Humanize Care. Moral Concerns versus Witnessed Benefits for the Elderly", Proceedings of the International Conference on Health Informatics (Healthinf), Lisbon, vol. 1, pp. 648-653.

Wada F., Longe O., Danquah P. (2012), "Action Speaks Louder than Words - Understanding Cybercriminal Behavior Using Criminological Theories", *Journal of Internet Banking and Commerce*, vol. 17, n. 1, http://www.arraydev.com/commerce/jibc/.

Wada K., Shibata T., Saito T., Tanie K. (2004), "Effects of Robot-assisted Activity for Elderly People and Nurses at a Day Service Center", Proceedings of the IEEE, vol. 92, n. 11, pp. 1780-1788, DOI: 10.1109/JPROC.2004.835378.

World Health Organisation (2016), *Global Strategy on Human Resources for Health: Workforce 2030* (April 2016).

Krug E.G., Dahlberg L.L., Mercy J.A., Zwi A.B., Lozano R. (2002), *World Report on Violence and Health*, Geneva, World Health Organization.

Yon Y., Ramiro-Gonzalez M, Mikton C, Huber M, Sethi D. (2018), "The Prevalence of Elder Abuse in Institutional Settings: A Systematic Review and Meta-analysis", *European Journal of Public Health*, vol. 29, n. 1, pp. 58-67, DOI: 10.1093/eurpub/cky093.

Young R., Zhang L., Prybutok V.R. (2007), "Hacking into the Minds of Hackers", *Information Systems Management*, vol. 24, n. 4, pp. 281-287.

Yunus R., Hairi N., Yuen C. (2017), "Consequences of Elder Abuse and Neglect: a Systematic Review of Observational Studies", Trauma, Violence and Abuse, vol. 20, n. 2, pp. 1-17.

Zani B., Selleri P., David D. (2003), "La comunicazione. Modelli teorici e contesti sociali", Roma, Carocci.

Zhang X., Tsai F.-S., Lin C.-C., Cheng,Y.-F., Lu K.-H. (2018), "Fraud, Economic versus Social- psychological Losses, and Sustainable E-auction", *Sustainability* (Switzerland), vol. 10, n. 9, 3130.