POLITECNICO
MILANO 1863

Politecnico di Milano

Computer Science and Engineering

Philosophical Issues of Computer Science

AA 2018-2019

I nuovi fattori di invisibilità

a cura di

Luca Grella

2 Luglio 2019

Indice

Abstract

L'evoluzione umana ha avuto un incremento esponenziale con lo sviluppo della tecnologia. Oggi la tecnologia è una risorsa fondamentale e necessaria. Lo sviluppo tecnologico e informatico ha, però, anche i suoi contro. I nostri dati sono in mano a singoli colossi. Si condivide tutto e un gestore del servizio che utilizziamo potrebbe sapere tutto di noi, ma noi, viceversa, potremmo avere problemi ad accedere ai nostri stessi dati. Tutto questo sviluppo (o inviluppo) tecnologico, aumentando i casi di *invisibility factor* (termine coniato da Moor riferendosi all'invisibilità di tutte quelle operazioni informatiche delle quali si è inconsapevoli in quanto essenti parte integrante, ad esempio, dell'elaborazione interna dei vari software), porta alla necessità di ampliare la *computer ethics*. Un esempio pratico è l'invisibilità della *profilazione*, diretta conseguenza a un'evoluzione delle metodologie di gestione dei dati. Ampliare la *computer ethics*, inoltre, permette l'espansione degli *invisibility factor* per applicare la teoria di Moor all'informazione odierna.

Introduzione

Negli ultimi decenni, il mondo dell'informatica e delle tecnologie dell'informazione sta assumendo sempre più importanza. Con esso si stanno sviluppando a pari passo molti problemi di natura etica. In questo documento affronterò un discorso riguardante lo sviluppo dell'etica, sottolineando la sua importanza nel contesto informatico, soffermandomi su alcuni esempi e particolarità appartenenti al campo dell'informatica odierna. Nello specifico il documento è composto da 4 capitoli più un quinto capitolo conclusivo. Il primo capitolo si occuperà di dare un quadro completo della *computer revolution* sulla base di quanto affermato da Moor in alcuni suoi scritti, descrivendo la suddivisione degli stage (periodi) e soffermandosi sul ruolo della *computer ethics* nell'ultimo stage, ossia quello in cui viviamo. Entrando nel vivo del documento, il secondo capitolo descriverà il *fattore di invisibilità* di Moor, parte fondamentale della mia tesi essendo, a mio parere, una delle chiavi centrali dello sviluppo della *computer ethics*. Il terzo capitolo, invece, affronterà il discorso dell'importanza della tecnologia e della gestione dei dati, sempre in chiave etica e sempre riadattandosi al discorso del *fattore di invisibilità* di Moor. Inoltre, saranno mostrati alcuni esempi molto attuali a sostegno della mia tesi. Infine, nell'ultimo capitolo e nella conclusione, verranno unite tutte queste informazioni per parlare di privacy, di *profilazione* e di come il *profiling* possa, non essendo riconducibile a nessuna delle categorie descritte da Moor, essere definito come nuovo esempio di *fattore di invisibilità*. Punto cardine di questa mia tesi è la necessità dell'ampliamento della definizione di *fattore di invisibilità*. Tutto ha un punto di partenza e, nel nostro caso, il punto di partenza è proprio ciò che ci ha resi quelli che siamo: l'evoluzione.

Capitolo 1

La nostra era: l'apice della *Computer Revolution*

L'evoluzione ha sempre portato l'uomo a dei bivi. Il dibattito principale su qualsiasi cosa possa portare cambiamento, che sia esso positivo o negativo, è quasi sempre di natura morale: "Ciò che mi fa stare meglio, posso ottenerlo tramite un processo giusto?", "Cosa è giusto e cosa è sbagliato?", "Il fine giustifica i mezzi?", "È eticamente corretto ciò che sto facendo?", "Anche se ritengo sia sbagliato ciò che sto facendo, è giusto farlo comunque, dato che mi porta beneficio (e/o magari porta beneficio anche alla comunità)?". Queste sono alcune delle classiche domande che prima o poi tutti ci poniamo nella vita, ma il discorso diventa ancora più interessante se queste domande andassimo ad applicarle, come anticipato prima, all'evoluzione umana. Nello specifico, l'evoluzione umana ha avuto un'accelerazione esponenziale nell'ultimo secolo e la motivazione è chiaramente l'introduzione della tecnologia in ogni ambito. La tecnologia, infatti, ha sempre avuto uno sviluppo ricorsivamente intrinseco; più ci evolviamo tecnologicamente, inventiamo e creiamo nuovi strumenti tecnologici, più lo sviluppo si velocizza, in quanto gli strumenti stessi da noi inventati ci vengono in aiuto. Quindi, maggiore è il numero di tecnologie a nostra disposizione, maggiore sarà la velocità con cui ne creeremo altre. Per questo motivo si può parlare di "accelerazione esponenziale" della nostra evoluzione, che negli ultimi anni è basata solo ed esclusivamente sulla tecnologia. Questa corsa allo sviluppo tecnologico, però porta a dei cambiamenti rapidissimi non solo nell'approccio alla ricerca del "nuovo" e del "migliore", ma anche nell'approccio etico. Il filosofo James H. Moor, da cui ho preso spunto per sviluppare la tesi che discuterò in questo documento, si sofferma, per parlare di etica riguardante lo sviluppo tecnologico, sulla *computer revolution*, e, in particolare, afferma che essa può essere suddivisa in 3 periodi: *introduction stage*, *permeation stage* e *power stage* (Moor 2001). Il primo si riferisce al periodo in cui è avvenuta l'introduzione delle tecnologie informatiche e in cui solo poche persone potevano averne accesso. Il secondo (durato tra il 1980 e il 2000 circa) è il periodo in cui è avvenuta la permeazione delle tecnologie informatiche all'interno della società e le persone hanno iniziato ad essere sempre più dipendenti da ogni dispositivo elettronico. Gli utenti hanno iniziato a diventare sempre più sofisticati e le tecnologie sempre più *user-friendly*. Solo recentemente siamo entrati nel terzo periodo, il *power stage*. Secondo Moor, quello in cui stiamo vivendo è anche l'ultimo periodo della *computer revolution*. Il giorno in cui le tecnologie informatiche diventeranno necessarie, ossia la base della nostra esistenza, è già arrivato, quindi il giorno in cui si concluderà il *power stage*, sarà anche il giorno che concluderà la *computer revolution*. Il *power stage* è un periodo che durerà per moltissimo tempo e che vedrà un enorme sviluppo sia a livello scientifico, che a livello etico. Dato che l'ambito etico riguardante lo sviluppo delle tecnologie informatiche è davvero vasto e, anno dopo anno, si sta sempre

di più ampliando, è stato necessario provvedere a creare una branca specifica dell'etica, chiamata *computer ethics*. Lo sviluppo di tecnologie informatiche sta diventando sempre più delicato e quindi necessita, senza ombra di dubbio, della *computer ethics*. Il *power stage*, quindi, non è altro che il periodo della *computer ethics*. La *computer ethics* non fu presa in considerazione quando lo sviluppo delle tecnologie informatiche era ancora agli albori per il semplice fatto che difficilmente si poteva prevedere sia uno sviluppo così rapido, sia la nascita di così tanti problemi etici derivati dall'evoluzione informatica (si provi ad esempio a pensare a quanti dilemmi sono nati con lo sviluppo dell'intelligenza artificiale). L'etica dell'informatica non potrà sicuramente rispondere ad ogni domanda, ma sicuramente può fissare dei paletti e descrivere un percorso da seguire per evitare di superare alcuni limiti che non dovrebbero mai essere superati, né ora, né in un futuro in cui potremmo iniziare a pensare come macchine, o in cui le macchine potrebbero iniziare a pensare come noi (ad oggi ci sono differenti scuole di pensiero, inoltre, sulla capacità di pensiero di una macchina. "Le macchine possono pensare? E se la risposta è no, potranno mai pensare?": queste sono alcune domande di cui la *computer ethics* si occupa). Si può dunque affermare che lo sviluppo della *computer ethics* è direttamente proporzionale allo sviluppo delle tecnologie informatiche. Si può quindi anche affermare che argomenti etici affrontati in passato possano subire delle modifiche ed essere riadattati a situazioni più attuali? Lo scopo di questo documento è proprio rispondere a questa domanda, in particolare prendendo come riferimento quanto detto da Moor e utilizzando come esempio il suo *fattore di invisibilità* (Moor 1985).

Capitolo 2

Una particolarità delle tecnologie informatiche: il *fattore di invisibilità*

Per capire appieno la teoria di Moor riguardante il *fattore di invisibilità* bisogna fare alcune precisazioni. Ad oggi la maggior parte delle operazioni informatiche sono invisibili. Cosa significa "invisibili"? Il discorso è molto vasto, ma io mi soffermerò solo su alcuni esempi che, da soli, possono far comprendere meglio il mio pensiero. Quando avviene un processo informatizzato la maggior parte degli utenti, ma a volte anche lo stesso programmatore, sono inconsapevoli di buona parte delle elaborazioni interne (se non di tutte). Per questo motivo si può parlare di operazioni informatiche "invisibili". Il discorso, così spiegato, può sembrare molto astratto, ma Moor afferma che esistono 3 tipi di invisibilità (Moor 1985) e affianca questo suo pensiero ad alcuni esempi pratici che esporrò. Inoltre, porterò altri esempi, non riconducibili a nessuna delle 3 categorie dei fattori di invisibilità di Moor, per affermare che gli *invisibility factor* possono essere diversi e le categorie ampliate a più di tre. Ovviamente questo è un discorso che può essere fatto a posteriori, in quanto, quando Moor formalizzò la sua teoria sui "fattori di invisibilità", gli esempi a cui farò riferimento, o non erano attuali, oppure, con le tecnologie di qualche decennio fa, non potevano neanche essere pensati o previsti. Il primo *fattore di invisibilità* è quello che viene definito "abuso invisibile". Esso si verifica in situazioni quali, per esempio: furto di informazioni personali in seguito ad un accesso non autorizzato (riconducibile ad una invasione della proprietà privata e della riservatezza altrui) e furto di un interesse in eccesso in banca. Nella maggior parte di questi casi, la vittima non si accorge di essere stata violata nemmeno dopo molto tempo e quindi l'aggettivo "invisibile" assume ancor più valore, nonostante esso possa già essere definito tale in seguito alla difficoltà di scoprire un "abuso invisibile" mentre viene eseguito. Il secondo *fattore di invisibilità* è costituito dai "valori di programmazione invisibili", ossia quei valori che sono incorporati in un programma per computer. In questo caso si fa riferimento al rapporto *user-programmer*, in quanto, il più delle volte, il programmatore formula giudizi sul valore di cosa può essere importante o meno per l'utente, decidendo cosa mostrare. Ciò che viene ritenuto poco importante, viene reso invisibile all'esecutore (la maggior parte dei valori incorporati nel programma finale, dunque, sono invisibile all'utente). Il terzo ed ultimo *fattore di invisibilità* è il "calcolo complesso invisibile". Potrebbe sembrare il meno importante, ma, se ci si ragiona bene, grazie ad esso si può comprendere quanto ci stiamo affidando, nel corso degli anni, alle tecnologie informatiche. Spesso per arrivare a risultati o output di qualsiasi natura e tipo, ci affidiamo a programmi che svolgono operazioni molto complesse. Sono quest'ultime che possono essere ricondotte a calcoli complessi invisibili. Perché? Esse non possono essere analizzate da un essere umano a causa della loro complessità.

Se dovessero esserci errori nel processo non potrebbero quindi essere identificati. Per questo motivo ci conviene "fidarci della macchina" e accettare il suo output come corretto senza poterlo verificare. Ovviamente tutti questi esempi sono molto attuali e le relative definizioni di *invisibility factor* funzionano anche oggi, ma questa suddivisione in 3 macro-categorie può sembrare molto stretta e insufficiente se applicata ad altri ambiti che si sono sviluppati solo negli ultimi anni. Per ovviare a questo problema e applicare la teoria di Moor all'informazione odierna bisogna procedere all'espansione dei tre *invisibility factor*.

Capitolo 3

L'informazione odierna: dall'importanza della tecnologia alla gestione dei dati

La tecnologia, come detto poco fa, ha iniziato a diventare importante a partire dall'inizio del *permeation stage*, ma ora si può affermare essere diventata parte fondamentale e necessaria della nostra esistenza. Un esempio pratico è la dipendenza che la maggior parte delle persone oggi ha nei confronti del proprio smartphone. All'interno di esso è praticamente racchiusa la nostra vita: media, contatti, conversazioni e dati personali riguardanti qualsiasi ambito, ma anche dati di cui a volte siamo inconsapevoli o consapevoli solo per metà: si provi a pensare ad esempio alla cronologia della localizzazione e quindi anche alle posizioni visitate più di frequente o addirittura alla nostra posizione attuale (ma di questo ne parlerò più avanti). Perdere uno smartphone senza backup sarebbe, in ogni caso, molto scomodo e, potendo prevederne lo smarrimento o, in generale, una futura possibilità di inutilizzo, chiunque prenderebbe provvedimenti in anticipo per evitare di perdere dati o rimanere senza smartphone. Questa precisazione è utile per introdurre un esempio a sostegno della mia tesi. L'importanza attuale della tecnologia si può notare anche a livello sociopolitico o economico. Perché? "Il 16 maggio il Presidente degli Usa Donald Trump ha firmato un documento che vieta a Huawei, di vendere ed installare le proprie infrastrutture negli Stati Uniti senza una specifica autorizzazione" *(www.focus.it)*. Sebbene sia stata una mossa politica per favorire gli Usa (in particolare le aziende statunitensi in contrapposizione a quelle cinesi), è molto interessante soffermarsi, non tanto sul "perché", ma quanto sul "come". Come posso colpire maggiormente una persona? Togliendogli ciò di cui non può fare a meno e, in questo caso, è proprio ciò che è avvenuto: il sistema operativo firmato Google smetterà di supportare i dispositivi Huawei a partire da agosto, mettendo in difficoltà gli utenti Huawei americani e non, che probabilmente passeranno ad altri marchi in seguito alla fidelizzazione avvenuta, anno dopo anno, dal sistema operativo di Google, che invece continuerà a funzionare su tutti gli altri dispositivi. Diventa molto interessante pensare a quali sarebbero le conseguenze se il blocco Usa a Huawei o altre aziende cinesi continuasse: gli utenti Huawei dovrebbero cambiare dispositivo (piuttosto che farne a meno) e questo sottolinea ancora una volta l'enorme dipendenza dalle tecnologie informatiche che si è espansa esponenzialmente negli ultimi anni. Due problemi che sono la diretta conseguenza di questa dipendenza (che ho ridotto all'uso dello smartphone, ma che vale per numerosi altri esempi) sono: la gestione dei nostri dati che abbiamo volontariamente condiviso e, come ho accennato prima, la creazione autonoma di dati di cui siamo all'oscuro o consapevoli solo per metà (per esempio il *tracking* delle nostre posizioni). In entrambi i casi la gestione dei dati è in mano a dei singoli colossi: Facebook, Google... La particolarità di questa situazione è che ognuno di noi

è consapevole del fatto che qualsiasi dato condiviso potrebbe non essere in buone mani (vedi lo scandalo Cambridge Analytica che ha coinvolto Zuckerberg e Facebook), ma in fin dei conti, nella maggior parte dei casi, la cosa non ci tange. Oggi condividiamo tutto e un gestore del servizio che utilizziamo, ipoteticamente parlando, potrebbe sapere qualsiasi cosa di noi, ma noi viceversa abbiamo accessi molto ridotti e vincolati, spesso anche ai nostri stessi dati o ai dati di un nostro parente stretto. Un esempio è il caso di Apple del 2016. Un padre, dopo la precoce morte del figlio ancora 13enne, ha richiesto l'accesso ai dati del suo smartphone, dimostrando che l'accesso gli veniva consentito dal figlio stesso quando era ancora in vita (a dimostrazione l'impronta digitale del padre salvata sul telefono, non più utilizzabile dopo 48 ore di inattività o dopo lo spegnimento poiché sostituita da un codice di blocco, in questo caso non conosciuto dal padre). Accesso che non è stato permesso da Apple per varie ragioni, sia di natura legale, sia di natura morale. Ora la questione è molto delicata: eticamente, moralmente e umanamente potrebbe sembrare più che lecita la richiesta del padre, ma bisogna prendere in considerazione anche altri aspetti che, sul momento e a caldo potrebbero passare in secondo piano. Per esempio "Cook precisò che forzare il codice criptato del cellulare, avrebbe costituito un precedente pericoloso. Questa è la realtà. Aprire una *backdoor* in quel telefono o in mille altri, significa minare la sicurezza delle tecnologie elaborate appositamente per proteggere i dati degli utenti, dati che possono essere più o meno sensibili, ma che rimangono comunque personali. Non è un caso se, in tal senso, molte piattaforme, come Facebook e Google, hanno reso disponibile una funzione che rappresenta un testamento digitale volontario dell'utente affinché egli possa assicurare l'accesso ai propri profili a persone puntualmente individuate" *(www.agi.it)*. Si può notare che ogni esempio sopra riportato fa sempre riferimento alla gestione dei dati. La gestione dei dati, a volte, non è però solo un servizio offerto al cliente che porta benefici a livello di ritorno economico, ma è una vera e propria fonte di interesse per il servizio stesso che la utilizza per profilare e creare un identikit vero e proprio dell'utente (questo identikit viene effettuato non solo grazie ai dati offerti liberamente dall'utente, ma anche dalla sua predisposizione a certi post, alle sue condivisioni e al suo tempo passato a utilizzare il servizio. Per esempio, il *profiling* potrebbe permettere di conoscere l'orientamento politico e religioso dell'utente, senza che, paradossalmente, egli l'abbia mai dichiarato pubblicamente o scritto da qualsivoglia parte). Unendo e triangolando i dati della *profilazione* di milioni di persone si possono ottenere informazioni riguardo a qualsiasi cosa e si possono effettuare delle indagini su scala globale. Spesso il *profiling* è legale, poiché i colossi che gestiscono i dati di milioni di utenti si muovono all'interno dei confini dettati dalla legge (a parti rari casi, come per esempio il già citato scandalo Cambridge Analytica), ma è eticamente giusto?

Capitolo 4

Il *profiling* come *invisibility factor*

Il *profiling* è forse l'esempio più interessante tra tutti quelli analizzati ed è quello che meglio descrive le nuove frontiere della tecnologia dell'informazione, ma è davvero qualcosa di negativo? Ritornando al pensiero di Moor, tutto questo sviluppo, o inviluppo (secondo i punti di vista), tecnologico porta a una necessità di ampliare la *computer ethics*. Il motivo principale riguarda tutte le branche dell'informatica. Un banale esempio, da tutti conosciuto, sono le intelligenze artificiali e la previsione che, in un futuro prossimo, possano arrivare ad avere una propria coscienza. La *computer ethics*, però, è necessaria non solo in questi casi estremi. Essa è il fondamento di ogni tecnologia informatica che si è sviluppata in passato, si sta sviluppando nel presente e che si svilupperà in futuro. Quindi la necessità di ampliare la *computer ethics* dipende solo da questo? No. La necessità di ampliarla è anche data dal fatto che, con lo sviluppo tecnologico e informatico, aumentano i casi di *invisibility factor* e, spesso, essi non possono più essere organizzati tramite la classificazione creata da Moor nel suo documento del 1985. Il *profiling* rientra, per me, negli esempi di nuovi casi di *invisibility factor*. Per spiegare il perché, bisogna innanzitutto capire: (1) se il *profiling* sia davvero qualcosa di negativo, (2) come sia visto dalla *computer ethics* e quindi intraprendere un discorso sull'importanza morale del commercio dei dati digitali e (3) se gli *invisibility factor* siano sempre qualcosa di negativo oppure ci siano delle eccezioni. Il *profiling* è nato molto prima dello sviluppo delle tecnologie informatiche ed è tuttora utilizzato in diversi ambiti. In qualsiasi situazione esso venga utilizzato, lo scopo del *profiling* è sempre lo stesso: inquadrare un individuo, ottenendo più informazioni possibili su di esso e studiarle creando un modello leggibile secondo gli standard ottenuti in precedenza, triangolando enormi quantità di dati, a loro volta prelevati da numerosi campioni. Ciò che cambia da ambito ad ambito è la motivazione che porta a utilizzare la tecnica del *profiling*. A seconda della motivazione, quindi, possiamo affermare se esso sia qualcosa di negativo o di positivo. Per esempio, il *profiling* è molto utile per analizzare i dati di un paziente in campo medico, accostando i suoi dati ai dati dei modelli già presenti nel sistema. È interessante soffermarsi un attimo su come la *profilazione* in campo medico sia direttamente collegata alla big data analytics. I termini big data e big data analytics sono spesso usati nel contesto dell'assistenza sanitaria come una frase onnicomprensiva che si riferisce all'uso di grandi set di dati. Il loro uso sempre più regolare apre la strada a potenziali equivoci etici e sociali (Floridi 2012). I big data sono definiti come raccolte di dati così grandi e complesse che la loro manipolazione e gestione richiede l'applicazione di una serie di tecniche di calcolo, incluso ma non limitato all'apprendimento automatico e all'intelligenza artificiale (Stuart Ward e Barker 2013). L'analisi dei big data è definita come "il processo di raccolta, organizzazione e analisi di

grandi insiemi di dati (chiamati big data) per scoprire pattern e altre informazioni utili" (Heymann e Rodier 2004). Oppure si può fare riferimento alla *profilazione* criminale: l'ultimo decennio ha visto l'emergere di tecniche di *profiling* nelle forze dell'ordine per prevedere e prevenire futuri crimini prima che si verifichino. Tutti esempi di situazioni in cui il *profiling* ha solo aspetti positivi. Ma possiamo dire lo stesso riguardo al discorso morale? È giusto che vengano utilizzati i dati di un paziente, che non ha dato il consenso per il trattamento di essi, per salvare la vita di un altro paziente? Per quanto riguarda il secondo esempio, invece, nel 2009, l'Istituto nazionale di giustizia ha negato queste tecniche di *profiling* come polizie predittive, il che implica prelevare dati da fonti disparate, analizzarli e quindi utilizzare i risultati per anticipare, prevenire e rispondere più efficacemente ai reati futuri. Attualmente il software di sorveglianza predittiva è impiegato in 25 dipartimenti di polizia di grandi dimensioni nelle città degli Stati Uniti. Ad oggi esistono due tipi di software: sistemi basati sul luogo che fanno previsioni su dove e quando si verificherà un crimine futuro e strumenti basati sulle persone che prevedono chi è probabile che commetta o sia vittima di reato. Entrambi i sistemi si basano su algoritmi per generare le previsioni a partire dalla *profilazione* e raccolta dati di crimini passati. La crescente prevalenza della polizia predittiva è un sito contemporaneo di preoccupazione per una serie di organizzazioni per i diritti civili, attivisti e teorici. Nel loro recente lavoro su *pre-crimine* e *big data policing*, McCulloch e Wilson (2016) e Ferguson (2017) evidenziano i problemi che la polizia predittiva pone alle libertà civili sotto forma di sorveglianza rafforzata, discriminazione razziale e pregiudizio. Questi programmi, sostengono, si basano in modo problematico su dati di crimine storico, che sono spesso misure inaccurate dei passati tassi di criminalità, per colpire i luoghi e le persone di possibili reati futuri. Il discorso è identico se ci spostiamo sulla *profilazione* degli utenti di un social network. I loro dati possono anche essere venduti a società che li utilizzeranno per il bene comune, ma gli utenti stessi ne sono a conoscenza? Il discorso del commercio dei dati digitali è per la *computer ethics* un argomento molto dibattuto e ad ora si può solamente affermare che la *profilazione* sia sicuramente etica solo nel caso in cui l'utente (1) dia il proprio consenso al trattamento dei propri dati consapevolmente (spesso viene fatto inconsapevolmente), (2) sappia esattamente di quali dati si stia parlando, ma soprattutto (3) conosca chi potrebbe accedervi. Se viene a mancare anche solo uno di questi punti, allora si può parlare di *invisibility factor*. Dato che è l'utente stesso ad aver fornito i dati, non c'è stato un accesso illegale, né tantomeno una violazione di proprietà privata. Per questo motivo questo *invisibility factor* non può essere accostato all'abuso invisibile, ma è qualcosa di totalmente nuovo. Altro esempio eclatante di nuovo *invisibility factor* è l'utente che viene profilato e tramite gli algoritmi di *profilazione* vengono ottenuti dati sensibili, o non, che non siano mai stati inseriti online né tantomeno autorizzati. Anche in questo caso non è avvenuto nessun "furto" in quanto i dati sono stati direttamente creati dall'algoritmo. Inoltre, numerosi casi hanno dimostrato che riuscire a dimostrare

l'illegalità in questo tipo di *profilazione* diventa quasi impossibile. Tutti questi sono esempi negativi di *invisibility factor*, ma non sempre un *invisibility factor* è qualcosa che danneggia l'utente. Per esempio, i "valori di programmazione invisibili" (seconda categoria di *invisibility factor* secondo Moor) talvolta non vanno a danneggiare l'utente, ma, al contrario, vanno a semplificare l'utilizzo del software o la lettura degli output.

Conclusioni

Per concludere possiamo affermare quindi che il *profiling* non è altro che un esempio diretto che può portare a un dibattito etico riguardante gli standard odierni sulla privacy. Inoltre, essendo direttamente coinvolto in questo discorso ho provato a portare una mia tesi riprendendo il pensiero di alcuni filosofi che hanno approfondito il discorso della *computer ethics* negli ultimi anni. Le questioni di etica e legalità sono essenziali in molti settori. Medici, insegnanti, funzionari governativi e uomini d'affari hanno tutti una supervisione legale ed etica per controllare come funzionano le loro professioni. La tecnologia dell'informazione, al contrario, non ha una standardizzazione generale in atto. Tuttavia, poiché la tecnologia dell'informazione diventa sempre più influente, le considerazioni etiche e legali diventano altrettanto pertinenti. La maggior parte delle persone ha i propri dati personali diffusi in tutto il mondo digitale. Anche le cose ritenute sicure, come account di posta elettronica o privati, sono accessibili da fonti non intenzionali. La maggior parte dei datori di lavoro controlla attivamente le abitudini dei loro dipendenti. La privacy ha implicazioni legali in evoluzione, ma ci sono anche considerazioni etiche. Le persone sanno come vengono monitorati i loro account? In che misura si verifica tale monitoraggio? I problemi di privacy possono facilmente diventare una china scivolosa, erodendo lentamente e completamente il diritto alla privacy di un individuo. I media digitali hanno permesso alle informazioni di fluire più liberamente di prima. Questo scambio di idee ha una reazione legale ed etica. Come si può stabilire la proprietà nel regno digitale? Le cose possono essere facilmente copiate e incollate online, il che rende difficile il controllo della proprietà intellettuale. Le nozioni legali come il copyright hanno faticato a tenere il passo con l'era digitale. Le aziende nel settore della musica e dell'intrattenimento hanno spinto per maggiori protezioni legali per le proprietà intellettuali, mentre altri attivisti hanno cercato di fornire maggiori libertà per lo scambio di idee nel regno digitale. A un certo livello, tutti sanno che le loro vite online sono monitorate. Gli Stati Uniti hanno persino approvato una legge che consente al governo di monitorare attivamente i cittadini privati in nome della sicurezza nazionale. Queste misure hanno riacceso un dibattito su quali informazioni possono essere raccolte e perché. Questo dibattito si applica anche su scala ridotta, perché le aziende devono considerare quali informazioni raccogliere dai propri dipendenti. Questo problema richiama due domande: le persone sanno quali informazioni vengono monitorate? Hanno il diritto di sapere come vengono utilizzati i loro dati? In passato, i problemi di sicurezza venivano risolti chiudendo una porta. La sicurezza digitale è molto più complicata. I sistemi di sicurezza per le reti digitali sono informatizzati per proteggere le informazioni vitali e le risorse importanti. Tuttavia, questa maggiore sicurezza è accompagnata da una maggiore sorveglianza. Tutti i sistemi di sicurezza hanno rischi intrinseci, il che significa che si tratta di quali rischi sono accettabili e quali libertà possono essere perse. In definitiva, i professionisti delle tecnologie infor-

matiche devono bilanciare il rischio con la libertà di creare un sistema di sicurezza che sia efficace ed etico allo stesso tempo. La neutralità della rete è diventata una questione di tendenza grazie agli sforzi legislativi negli ultimi anni. La questione della neutralità della rete è essenzialmente una questione di accesso. I fautori vogliono che Internet rimanga aperto a tutti mentre alcune aziende vogliono creare un accesso a più livelli per coloro che sono disposti a pagare. Il problema si estende anche all'uso privato di Internet poiché il costo del servizio in alcune aree potrebbe essere proibitivo. La più ampia questione etica è se lo scambio digitale sia o meno un diritto universale. Il costo dell'accesso può ostacolare la crescita del business, lo spirito imprenditoriale e l'espressione individuale. Questi problemi sono essenziali per tutti, ma hanno un peso extra per coloro che lavorano con le tecnologie dell'informazione. È importante ricordare che lavorare con la tecnologia non è separato dai contesti etici, ma può effettivamente aiutare a definire un codice legale ed etico per le generazioni a venire. Ho voluto ampliare il *profiling* come discorso pratico, per portare un esempio di come gli *invisibility factor* di Moor siano oggi insufficienti. Inoltre, tutti gli esempi riguardanti il discorso della privacy sopracitati, possono essere letti in chiave di *invisibility factor*. Tutto ciò che è futuro, può essere letto e interpretato in chiave passata e la privacy non si discosta da questo discorso: *"Privacy is in modern societies an ideal rooted in the Enlightenment"* (Fuchs 2010). È bello poter pensare al futuro come qualcosa che viene costruito, giorno dopo giorno, su solide basi. Quelle basi dipendono dal presente, dipendono dal nostro pensiero e dalle nostre idee, dipendono da noi. Tutto ciò che noi siamo lo dobbiamo a ciò che ci è stato trasmesso dal passato. Tutto ciò che è passato, in chiave riadattata, può essere applicato a ciò che ci circonda oggi o a ciò che verrà: spero di averlo trasmesso con questo breve documento, esprimendo quanto, un'idea di più di 30 anni fa, possa essere così attuale.

Riferimenti

Libri e Articoli

- Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement.
- Floridi, L. (2005). The ontological interpretation of informational privacy. Ethics and Information Technology 7:185–200.
- Floridi, L. (2012). Big data and their epistemological challenge. Philosophy and Technology, 24(4), 435–437.
- Fuchs, C. (2010). StudiVZ: social networking in the surveillance society. Ethics Inf Technol 12:171–185.
- Heymann, D. L., & Rodier, G. R. (2004). SARS: a global response to an international threat. Journal of World Affairs, 10(2), 185–197.
- Loi, M. & Christen, M. (2019). Two Concepts of Group Privacy. Philosophy & Technology.
- McCulloch, J., & Wilson, D (2016). Pre-crime: Pre-emption, precaution and the future.
- Mittelstadt, B. (2017). From Individual to Group Privacy in Big Data Analytics. Philos. Technol. 30:475–494.
- Moor, J. H. (2001). The future of computer ethics: You ain't seen nothin' yet!. Ethics and Information Technology 3: 89–91.
- Moor, J. H. (2005). Why we need better ethics for emerging technologies. Ethics and Information Technology (2005) 7:111–119.
- Moor, J. H. (1985). What is Computer Ethics. Metaphilosophy 16(4):266 – 275.
- Stuart Ward, J. and Barker, A. (2013). Undefined by data: A survey of big data definitions. arXiv:1309.5821v1.
- Turilli, M. & Floridi, L. (2009). The ethics of information transparency. Ethics Inf Technol 11:105–112.
- Wallace, K. A. (1999). Anonymity. Ethics and Information Technology 1: 23–35.
- Winter, J. S. (2014). Surveillance in ubiquitous network societies: normative conflicts related to the consumer in-store supermarket experience in the context of the Internet of Things. Ethics Inf Technol 16:27–41.

Siti web

- www.agi.it
- www.focus.it
- www.springer.com

