Lavoro di gruppo di:

Alessandro Daffonchio

Debora Alexandra Drugan

Sara Galvan

Filippo Pingitore

Matilde Serra

Le problematiche legate alla Privacy

1. COS'È LA PRIVACY?

Non limitandosi allo scopo per il quale sono stati originariamente creati – connettere più facilmente e rapidamente le persone tra loro al fine ultimo, come suggerisce il nome, di socializzare – i social network si sono progressivamente trasformati in strumenti di lavoro, svago o divertimento a seconda dei casi e delle esigenze. Le informazioni contenute in essi pongono tuttavia diversi problemi relativi alla privacy.

Con il termine “privacy” si intende il diritto di una persona di poter mantenere riservate le informazioni riguardanti la propria vita privata.

Occorre specificare che il diritto alla privacy non va confuso con il diritto al segreto (quello che prevede, ad esempio, che un medico abbia l’obbligo di mantenere il segreto professionale sulle cartelle cliniche dei suoi pazienti) e nemmeno con il diritto alla protezione dei dati personali, che concerne le notizie relative alla vita dell’individuo. Una telecamera posizionata da qualcuno all’interno di un’abitazione privata sarebbe perciò una violazione della privacy, mentre la diffusione di informazioni personali, sarebbe una diffusione impropria dei dati.

2. LE SANZIONI IN CASO DI VIOLAZIONE AL DIRITTO ALLA PRIVACY

I rischi cui si può incorrere in caso di violazione della privacy sono molto elevati e sottovalutarli potrebbe costare caro agli individui o agli enti inadempienti.

Eventuali violazioni possono comportare infatti conseguenze rilevanti: le autorità di controllo, secondo quanto affermato nell'articolo 83 del "Regolamento generale sulla protezione dei dati" dell'Unione Europea, hanno il potere di infliggere sanzioni amministrative pecuniarie fino a 20 milioni di euro o, per le imprese, pari al 4% del fatturato totale annuo.

Nel decidere la tipologia di sanzione da comminare, le autorità di controllo devono tenere conto di diversi elementi, tra cui:

- la natura, la gravità e la durata della violazione;
- il carattere doloso o colposo della violazione;
- il grado di responsabilità;
- eventuali precedenti violazioni;
- le categorie di dati personali interessate dalla violazione;
- la maniera in cui l'autorità di controllo ha preso conoscenza della violazione;
- eventuali altri fattori aggravanti o attenuanti.

Queste sanzioni possono portare a gravi conseguenze, come ad esempio: la limitazione, la sospensione o addirittura il blocco dei profili su internet, ma anche sanzioni penali.

Con “violazione dei dati personali”, anche definita *Personal Data Breach*, si intende una violazione della sicurezza che causa, in maniera accidentale o volontaria, la perdita, la modifica, la distruzione, la divulgazione non autorizzata o l’accesso ai dati personali.

La Personal Data Breach può essere causata, per esempio, da:

- Infedeltà aziendale. Una persona interna all’azienda con autorizzazione ad accedere ai dati personali può farne copia e divulgarli pubblicamente;
- Accesso abusivo. Un individuo accede ai dati sensibili di un’altra persona in maniera non autorizzata e divulga quanto acquisito;
- Il furto. La sottrazione di strumenti tecnologici come un notebook può portare all’accesso, tramite questo, ai dati personali dell’individuo derubato;
- Perdita accidentale. Una persona che smarrisce un dispositivo come una chiavetta USB si espone alla violazione dei dati personali.

3. LE POSSIBILI VIOLAZIONI

I problemi più comuni riguardanti la violazione della privacy riguardano però la diffamazione, il cyberbullismo e altri fenomeni che sono in crescita negli ultimi anni. E’ sempre più frequente, infatti, il furto di dati, sia da parte di hacker – che, manomettendo il sistema, ottengono informazioni su dati personali o carte di credito – sia proprio da parte dei social.

Un esempio famoso, ormai passato alla storia contemporanea, è il caso Facebook. Cosa è successo? L’invenzione di Mark Zuckerberg è stata accusata di aver rubato i dati di ben 87 milioni di americani e di averli usati, ovviamente per guadagnare, ma anche per influenzare la politica degli Stati Uniti. Lo scandalo dei dati Facebook-Cambridge Analytica è stato uno dei maggiori

scandali politici avvenuti all'inizio del 2018, quando fu rivelato che Cambridge Analytica aveva raccolto i dati personali di milioni di account Facebook senza il loro consenso e li aveva usati per scopi di propaganda politica. Esso ha provocato un forte calo del prezzo delle azioni di Facebook, alla quale venne chiesta una regolamentazione più rigorosa sull'uso dei dati personali degli utenti. L'evento fu significativo in quanto accese i riflettori sugli standard etici dei social media, delle organizzazioni per la consulenza politica, e degli stessi politici. I sostenitori dei consumatori hanno chiesto una maggiore protezione degli utenti online e in materia di diritto alla privacy, oltre a limitare la disinformazione e la propaganda.

Inoltre, come possiamo dimenticare i dati che ci chiede quotidianamente Google, il motore di ricerca più usato al mondo? Quest'ultimo raccoglie senza sosta una mole impressionante di informazioni, fra posizioni, elenchi di ricerche, preferenze sulle scelte d'acquisti, ecc.

Anche il servizio di messaggistica più popolare al mondo, WhatsApp, è periodicamente coinvolto in scandali che riguardano il furto di dati, poiché chiede agli utenti di rendere pubblico un dato così sensibile come il numero di telefono.

Innumerevoli sono poi le violazioni della privacy "di minore entità", in quanto a dati rubati, ma altrettanto pericolose per chi le subisce. Non è difficile infatti, navigando in rete, sentire di utenti che vengono truffati da pubblicità promettenti come: "Registrati e guadagnerai 49 milioni di euro subito!", che, se analizzate razionalmente, sono ovviamente truffaldine, ma che, all'occhio dell'utente inesperto, possono sembrare convenienti e vantaggiose.

Sulla rete capita anche a molte persone di "accettare" i cosiddetti "Cookies", oppure di "rivedere le proprie scelte" nell'account. Tutto ciò ruota intorno al fatto che si seguirà quasi sempre la via più semplice, ossia accettare la proposta per poter accedere liberamente ai contenuti di un sito. Un altro esempio sono i contratti delle compagnie telefoniche spesso firmati alla cieca, senza leggere attentamente nel dettaglio ciò che essi propongono.

4. CONSIGLI PER UN USO CORRETTO E APPROPRIATO

La consapevolezza di ciò che si pubblica e la corretta comprensione di ciò che vediamo e leggiamo stanno alla base di un uso corretto e sicuro di Internet. Esistono modi, anche attraverso il ricorso alle vie legali se serve, per difendersi sui social.

La navigazione in rete può essere tranquillamente protetta con pochi accorgimenti, tra cui i VPN o gli antivirus. I secondi hanno una funzione ovvia, ma i primi sono anche più utili. Un VPN è un servizio in grado di proteggere la navigazione sulla rete, da virus e truffe, ma non solo: permette anche di impostare la navigazione da un paese all'altro, in modo da poter, ad esempio, osservare i siti non disponibili nel nostro paese o sfogliare cataloghi di prodotti mediatici non ancora usciti. Oppure, all'opposto: consente di continuare a "navigare" in Italia, anche se fisicamente si è in un altro paese. In più, ci sono molti comportamenti che ogni utente può seguire per la salvaguardia di se stesso e alternative molto più sicure ai social più noti e utilizzati. Il primo consiglio è, per chi usa ad esempio Instagram o Facebook, di non nutrire la fame di dati delle piattaforme e degli utenti "cattivi" – e, insieme, il nostro ego! – continuando a postare contenuti sulla propria vita privata. Nessun problema se si usa il proprio nome reale come tag o le proprie foto, ma si dovrebbe cercare ad esempio di:

- Non registrarsi con il proprio numero (è preferibile una mail).
- Non dare troppe informazioni sugli acquisti, o sugli spostamenti effettuati.
- Valutare con attenzione ogni richiesta "redditizia" che compare nei DM.

Dare troppe informazioni, non solo ci rende più vulnerabili al furto di dati, ma può seriamente danneggiare la nostra sicurezza. Non è raro infatti ricevere chiamate, link, o messaggi spam per aver commesso la leggerezza di diffondere un numero pubblico. È meno frequente, ma altrettanto pericoloso, incontrare

problemi nella vita reale, come il fenomeno dello stalking, perché si sono date troppe informazioni sui propri spostamenti.

Per quanto riguarda la diffusione di materiale privato e "sensibile", come foto e video intimi, anche se non è espressamente vietato dalla legge produrre questi contenuti, è comunque fortemente sconsigliabile inviarli ad altre persone, anche ad amici e fidanzati. In ogni caso, è stata finalmente approvata una legge per il reato di diffusione di questi materiali, conosciuta come legge sul *Revenge porn*. Se mai si dovesse subire una violenza legata a questo reato grave, la cosa migliore da fare sarebbe informare subito le forze dell'ordine e mostrare, senza vergogna, ogni prova a disposizione.

5. ALTERNATIVE SOCIAL?

Sarebbe importante parlare anche delle possibili alternative ai vari social "tradizionali". Un consiglio riguardante Whatsapp è quello di ridurre il suo utilizzo al minimo indispensabile, per comunicare, ad esempio, sui gruppi classe o con amici che non possiedono altri social. Alternative decisamente migliori per altri scopi sono: Telegram, che combina efficienza, funzionalità innovative (come bot che scaricano la musica direttamente da Spotify) e rispetto della privacy. Ciò che si nota subito in questa app è che il numero è occultabile. Questo è fondamentale per difendere l'utente dalla maggior parte delle minacce. Bisogna infatti ribadire che il numero di telefono sui social è importante quanto il nome! Un'altra opzione è Discord, applicazione studiata per chat vocali e di testo, con infinite possibilità.

I social sono una delle invenzione a maggior impatto sociale del secolo e rifiutarli *a priori* significherebbe rifiutare un pezzo di socialità. Ma, siccome le insidie presenti in rete non si rivelano inferiori a quelle che minacciano la nostra esistenza nel "mondo reale", occorre essere sempre vigili e consapevoli nel loro impiego.

6. “TO BE LET ALONE”

Il 21 agosto 2019 è scomparso uno tra i maggiori esperti di diritto delle nuove tecnologie, un garante europeo della privacy: Giovanni Buttarelli. Egli ha seguito l'*iter* della legge che per la prima volta ha introdotto nel sistema legislativo italiano il principio della tutela dei dati personali. Buttarelli ha continuato a occuparsi di tutela della riservatezza a livello europeo nel ruolo di Garante europeo della protezione dei dati.

La tutela dei dati personali è riconosciuta oggi come un diritto dell'individuo ad avere il controllo sulle informazioni relative alla propria persona, ma la sua storia ha radici nell’Ottocento. Il diritto “to be let alone” nasce infatti negli Stati Uniti nel 1890 e viene poi elaborato in Italia a partire dagli anni ‘60-'70 del Novecento come “diritto alla libertà nello svolgimento della propria personalità”.

Il diritto alla privacy, nel percorso che ha portato alla nascita della Costituzione Italiana, entrata in vigore nel 1948, non era al centro della discussione. Tuttavia un primo e importante accenno alla privacy è riscontrabile nell'articolo 2 della Costituzione, che incorpora la privacy nei diritti inviolabili dell'uomo, come anche nel 1973 ha sostenuto la Corte Costituzionale con la sentenza n. 38.

In Europa, l'Italia ha approvato nel 1996 la legge 675 che ha introdotto una legge di tutela della privacy. Il 4 maggio 2016 è stato pubblicato in Gazzetta Ufficiale il Regolamento UE 2016/679 del Parlamento Europeo, per migliorare la protezione dei dati personali dei cittadini europei dentro e fuori l'Unione.