مقاله

مجلهٔ

پژوهشهای حقوقی

علمی ـ ترویجی

شماره ۲۳

هزار و سیصد و نود و دو ـ نیمسال اول

شهر دانش

مؤسسه مطالعات و پژوهشهای حقوقی

http://jlr.sdil.ac.ir/article_32833.html

مجله پژوهشهای حقوقی (علمی ـ ترویجی)، شماره ۲۳، نیمسال اول ۱۳۹۲
صفحات ۱۱۳ الی ۱۳۷، تاریخ وصول: ۱۳۹۱/۶/۷، تاریخ پذیرش: ۱۳۹۱/۹/۲۷

حریم خصوصی در شبکه‌های اجتماعی مجازی

باقر انصاری* ـ شیما عطار**

چکیده: امروزه شبکه‌های اجتماعی مجازی همچون فیس بوک، مای اسپیس و توییتر شهرتی جهانی یافته و به بخش مهمی از زندگی مدرن تبدیل گشته‌اند. میلیون‌ها نفر در سراسر جهان، عضو این شبکه‌ها شده و انبوهی از اطلاعات خود را روزانه در این شبکه‌ها منتشر می‌سازند. اطلاعاتی که کاربران در این شبکه‌ها منتشر می‌کنند ممکن است از سوی گردانندگان شبکه‌ها یا اشخاص ثالث مورد سوء استفاده قرار گیرد. برای مثال، از اطلاعات خصوصی آن‌ها در فضای مجازی افشا شود یا برای مقاصد تبلیغاتی در اختیار شرکت‌ها قرار گیرد یا برای مزاحمت‌های مختلف استفاده شود. از این‌رو، شبکه‌های مذکور به سکوی دسترسی آسان به داده‌های اشخاص تبدیل شده‌اند وداده‌های شخصی کاربران و برخی افراد مرتبط با آن‌ها در این شبکه‌ها مورد تهدید قرار گرفته است. برای مقابله با این تهدیدها، تلاش‌هایی در سطح بین‌المللی و ملی آغاز شده است ولی به نتایج مطلوب و قابل اتکایی نرسیده است. در کشور ما نیز با اینکه تهدیدهای ناشی از این شبکه‌ها دامنگیر بعضی کاربران شده است متأسفانه نگرانی از نقض حریم خصوصی از سوی این شبکه‌ها یا اشخاص مرتبط با آن‌ها هنوز به یک نگرانی جدی تبدیل نشده است. از این‌رو، مقاله حاضر تلاش کرده است تا ابتدا مفهوم شبکه‌های اجتماعی مجازی و نحوهٔ

* عضو هیأت علمی دانشکده حقوق دانشگاه شهید بهشتی Email: ansari126@hotmail.com
** دانشجوی کارشناس ارشد حقوق ارتباطات، دانشکده حقوق دانشگاه علامه طباطبایی

فعالیت آن‌ها را تبیین کند (بخش اول)، سپس تهدیدهای ممکن از ناحیهٔ عضویت در این شبکه‌ها علیه حریم خصوصی افراد و تدابیری را که تاکنون برای حمایت از افراد در برابر این تهدیدها وجود دارندمطالعه کند(بخش دوم).
کلیدواژه‌ها: شبکه‌های اجتماعی مجازی، حریم خصوصی، داده‌های شخصی، مزاحمت‌های مجازی.

مقدمه

امروزه بسیاری از فعالیت‌های افراد به صورت آنلاین انجام می‌شود. اینترنت امکان تبادل همزمان اطلاعات را ممکن ساخته است. شبکه‌های اجتماعی مجازینیز بخشی از اینترنت هستند. این شبکه‌ها پدیده قرن بیست‌ویک هستند که به افراد امکان دستیابی به اطلاعات دیگران و برقراری ارتباطات جدید را ضمن حفظ روابط گذشته فراهم می‌آورند. شبکه‌های مذکور بیش از هر چیز به افراد اجازه می‌دهند شبکه‌ای از ارتباطات برای خود ایجاد کنند؛ بدین معنا که پس از ساختن پروفایل[1] در یک شبکه بتوانند با سایر کاربران آن شبکه ارتباط برقرار کنند.

شبکه‌های اجتماعی مجازی به سرعت به مسیری هموار برای تعاملات اجتماعی تبدیل شده‌اند و این امکان را برای کاربران فراهم آورده‌اند که به سه طریق با یکدیگر به تعامل بپردازند: نخست، از طریق پروفایلی که کاربر به واسطهٔ آن خود را به دیگران معرفی می‌کند؛ این پروفایل، صفحه اینترنتی است[2] که دربردارنده اطلاعات فرد از جمله نام و نام خانوادگی، محل سکونت و تحصیل، سلایق، سرگرمی‌ها و غیره است؛ دوم، از طریق به اشتراک گذاشتن فیلم‌های ویدئویی، تصاویر، موسیقی و وب‌سایت‌های مورد علاقه و سوم از طریق ارسال پیام‌های عمومی و خصوصی.[3]

در این میان، علت اصلی گرایش به شبکه‌های اجتماعی مجازی، حفظ روابط دوستانه گذشته وبرقراری ارتباطات جدید است. مدیران این شبکه‌ها نیز مدعی‌اند که ماموریت آن‌ها اتصال شفاف‌تر مردم جهان به یکدیگر است.

این شبکه‌ها به بخشی از زندگی روزمره بسیاری از افراد تبدیل شده‌اند و مسایل جدیدی را برای رشته‌های مختلف مطالعاتی خصوصاً رشته حقوق ایجاد کرده‌اند. برای مثال، یک کاربر فیس‌بوک یا مای‌اسپیس ممکن است ۷۰۰ دوست در سراسر جهان در

1. Profile
2. Web page
3. Landis, "Friending our Users: Social Networking and Reference Services", p. 2.

فهرست دوستان خود داشته باشد و این امر ممکن است دام‌ها وخطرات زیادی را به ویژه برای حریم خصوصی افراد ایجاد کند.شبکه‌های اجتماعی، ابزارها و امکاناتی را در اختیار کاربران قرار می‌دهند تا آن‌ها بتوانند تصاویر، فیلم‌های ویدیویی و داده‌های خصوصی خود را در صفحه شخصی قرار دهند. با توجه به اینکه این شبکه‌ها امکان دسترسی افراد مختلف را به این اطلاعات فراهم می‌آورند، مسأله حمایت از حریم خصوصی به یکی از چالش‌های مطرح در خصوص این شبکه‌ها تبدیل شده است. با افزایش محبوبیت شبکه‌ها، تهدیدها علیه حریم خصوصی افراد هم افزایش یافته است.

با توجه به اینکه شبکه‌های اجتماعی مجازی بیشتر درمیان جوانان و نوجوانان رواج یافته‌اند می‌توانند آسیب‌پذیری این گروه‌های اجتماعی را افزایش دهند؛ برای مثال، فیس‌بوک تا مارس ۲۰۱۱ ششصد و چهل میلیون کاربر داشته‌است و کاربران عادی این شبکه روزانه ۲۰ دقیقه از وقت خود را در شبکه می‌گذرانند و ۲/۳ از کاربران نیز حداقل یک بار در روز به صفحه خود مراجعه می‌کنند.[۴]

در ایران نیز با گسترش عضویت در شبکه‌های اجتماعی مجازی، سوءاستفاده از داده‌های خصوصی افراد به قصد اخاذی و سایر مقاصد نامشروع افزایش یافته است. به دو نمونه از این سوءاستفاده‌ها اشاره می‌شود:

فردی در گیلان با سرقت هویت و عکس شهروندان از فیس‌بوک و ساخت ایمیل جعلی با هویت و تصویر آنان از طریق اتاق‌های گفت‌وگو با کاربران اینترنتی ارتباط برقرار کرده و برای استمرار دوستی‌های نامتعارف مجازی، تقاضای خرید شارژ و ارسال آن را می‌کرد و ضمن دریافت شارژ و اعلام یک شماره تلفن صوری، کاربران را فریب داده و بدین ترتیب مبلغی بالغ بر چهار میلیون ریال شارژ از ۲۰۰ کاربر اینترنتی، به صورت نامشروع تحصیل کرده بود. وی در اریبهشت ۱۳۹۱ توسط پلیس فتای گیلان (پلیس فضای تولید و تبادل اطلاعات) دستگیر شد.[۵]

مثالی دیگر، دستگیری جوانی باج‌گیر در تهران در اردیبهشت ۱۳۹۱ است که از طریق دوستی اینترنتی با دختران جوان در شبکه‌های اجتماعی مجازی، تصاویر خصوصی آن‌ها را به دست می‌آورد و پس از مدتی با تهدید به انتشار این تصاویر از

4. Tsaoussi, "Facebook, Privacy and the Challenges of Protecting Minors on Social Networking Sites", pp. 1-2.

۵. برای مطالعه بیشتر، نک: http://www.tabnak.ir/fa/news/240080.

این افراد اخاذی می‌کرد.[۶]

با توجه به مطالب فوق، هدف این مقاله آن است که تهدیدهای شبکه‌های اجتماعی مجازی علیه حریم خصوصی افراد را مورد مطالعه قرار دهد. بدین‌منظور، در بخش نخست، مفهوم شبکه‌های اجتماعی مجازی، چگونگی ایجاد و گسترش شبکه‌های اجتماعی مجازی و انواع شبکه‌ها به لحاظ موضوع، روند عضویت و ترکیب کاربران توضیح داده می‌شود. در بخش دوم نیزتهدیدهای موجود علیه حریم خصوصی افراد در شبکه‌های اجتماعی مجازی به ویژه تهدیدهای موجود علیه داده‌های شخصی کاربران (جمع‌آوری، استفاده، پردازش، افشا و ...) و مزاحمت‌های مجازی تبیین می‌شود.

بخش اول: مفهوم و انواع شبکه‌های اجتماعی مجازی

بند اول: مفهوم شبکه‌های اجتماعی مجازی

الف) چگونگی ایجاد و گسترش شبکه‌های اجتماعی مجازی

ظهور شبکه‌های اجتماعی مجازی به اواخر دهه ۱۹۹۰ باز می‌گردد.نخستین سایت‌های اجتماعی در اینترنت، به‌صورت اجتماعات آنلاین[۷] آغاز بکار کردند که از جمله آن‌ها می‌توان به Theglobe.com و Geocities در سال ۱۹۹٤ و Tripod در سال ۱۹۹۵ اشاره نمود. تمرکز این اجتماعات بر گردهم‌آوری اشخاص برای آشنا کردن آن‌ها با یکدیگر در اتاق‌های گفت‌وگو[۸]، به اشتراک گذاشتن اطلاعات و عقاید شخصی پیرامون یک موضوع به کمک ابزارهای شخصی پخش و انتشار همچون بلاگ‌ها[۹] بود.[۱۰]

اولین شبکه اجتماعی مجازی شناخته شده به نام www.SixDegrees.com در سال ۱۹۹۷ به وجود آمد که پس از ٤ سال بسته شد.[۱۱] شبکه مذکور این امکان را برای کاربران ایجاد می‌کرد که با ساختن پروفایل، فهرستی از دوستان خود تهیه کنند؛ البته پیش از اینینز برخی سایت‌های اجتماعی همانند www.classmates.com وجود داشت اما این اولین بار بود که کاربر می‌توانست امتیازات زیادی را همزمان داشته باشد. با این‌حال، بسیاری از شبکه‌های اجتماعی مجازی از سال ۲۰۰۳ به بعد پا به عرصه

---

٦. برای مطالعه بیشتر، نک: http://www.alef.ir/vdcauen6w49nmu1.k5k4.html?153220.

7. En ligne
8. Salles de discussion, Chatroom
9. Blogues
10. Collée, "Sécurité et vie privée sur les réseaux sociaux", p. 15.
11. Landis, Ibid, p. 3.

گذاشته‌اند؛ با ورود مای‌اسپیس و فیس‌بوک میلیون‌ها نفر جذب این شبکه‌ها شده‌اند و امروزه بیش از ۳۵۰ شبکه با میلیون‌ها کاربر وجود دارد.[۱۲] معروف‌ترین شبکه، فیس‌بوک است که در سال ۲۰۰٤ توسط دانشجوی هاروارد *مارک زوکربرگ*[۱۳] ایجاد شد. در ابتدا، تنها دانشجویان هاروارد و سپس کلمبیا، ییل و استنفورد می‌توانستند به عضویت این شبکه‌اجتماعی مجازی درآیند. از سال ۲۰۰٦ استفاده از آن برای عموم آزاد شد و امروزه برای هر کس که دارای پست الکترونیک معتبر و بیش از ۱۳ سال سن باشد قابل استفاده است. موفقیت فیس‌بوک چشمگیر بوده است؛ تنها یک سال پس از راه‌اندازی یک میلیون کاربر جذب این شبکه شدند؛ پنج سال بعد در فوریه ۲۰۰۹ تعداد کاربران به بیش از ۱۷۵ میلیون[۱۴] و سال ۲۰۱۰ به بیش از ۵۰۰ میلیون کاربر در جهان رسید[۱۵] و هم اکنون با بیش از ۸۰۰ میلیون نفر کاربر، از لحاظ جمعیت، عنوان سومین کشور پرجمعیت دنیا را به خود اختصاص داده است.[۱۶]

برخی دیگر از شبکه‌های اجتماعی مجازی مطرح به ترتیب تاریخ ایجاد عبارتند از: *لایوژورنال*[۱۷]، *اشین اونو*[۱۸] و *بلک پلنت*[۱۹] در سال ۱۹۹۹، *فرندزتر*[۲۰] و *اسکای بلاگ*[۲۱] در سال ۲۰۰۲، *لینکداینو مای اسپیس* در سال ۲۰۰۳، *اورکات*، *فلیکر*[۲۲] و *فیس‌بوک* در سال ۲۰۰٤، *یاهو ۳٦۰*[۲۳] و *یوتیوب* در سال ۲۰۰۵و *توییتر* در سال ۲۰۰٦. در این بین، به ترتیب *فیس‌بوک*، *توییتر*، *لینکداین*، *مای‌اسپیس*، *گوگل‌پلاس*[۲۴]، *دویانارت*[۲۵]، *لایوژورنال*، *تگد*[۲٦]، *اورکات*[۲۷]، *کافه مام*[۲۸]، *نینگ*[۲۹]، *میت‌آپ*[۳۰]، *مای‌لایف*[۳۱]، *مای‌یر*

12. Aldinge, "Social Networking Sites: How they are used to Perpetrate Criminal Activity and how Law Enforcement uses them as an Investigative Tool", p. 8.
13. Mark Zuckerburg
14. Tuunainen, Pitkänen & Hovi, "Users' Awareness of Privacy on Online Social Networking sites – Case Facebook", p. 2.
۱۵. آماری که در انتهای فیلم شبکه *اجتماعی* آمده است.
The Soial Network, directed by David Fincher, written by Aaron Sorkin and distributed by Columbia Pictures, 2010, USA.
16. Milivojevic, "Social Networking Sites and Crime: Is Facebook more than just a Place to Procrastinate?", p. 2.
17. Livejournal
18. AsianAvenue
19. BlackPlanet
20. Friendster
21. Skyblog
22. Flickr
23. Yahoo360
24. Google Plus+
25. DeviantART
26. Tagged
27. Orkut
28. CafeMom
29. Ning
30. Meetup

بوک[۳۲] و *بادو*[۳۳] عنوان ۱۵ شبکه اجتماعی مجازی محبوب تا ماه مه ۲۰۱۲را به خود اختصاص داده‌اند.[۳۴]

ب) تعریف شبکه‌های اجتماعی مجازی

شبکه اجتماعی مجازی از سه عنصر تشکیل شده‌است: شبکه، اجتماعی و مجازی.

در علم کامپیوتر، شبکه[۳۵] این‌گونه تعریف شده است: «سیستم ارتباطی بین کامپیوترها که امکان به اشتراک‌گذاشتن نرم‌افزارهای کاربردی را فراهم می‌آورد. شبکه محیطی است که کاربران مختلف می‌توانند با یکدیگر ارتباط برقرار نمایند و داده‌ها را به یکدیگر انتقال دهند یا از هم دریافت نمایند.»[۳۶]

تعریفی موسع از واژه *اجتماعی*[۳۷] نیز عبارت است از: «بیان وجود ارتباطات میان اشخاص زنده». این تعریف مرتبط است با زندگی افراد در جامعه، ارزش‌ها، معیارها و رفتار افراد و مطالعه روند تعامل میان افراد و گروه‌ها که سازگاری با جامعه، توسعه فرهنگی و بهبود شرایط اجتماعی را تسهیل می‌بخشد.[۳۸]

منظور از مجازی، «هر نوع ارتباطی است که با زبان رایانه انجام شود.»

بنابراین، شبکه *اجتماعی مجازی*[۳۹] را نیز این‌گونه تعریف می‌کنیم: «خدمات مبتنی بر وب که به افراد اجازه ساختن پروفایلی عمومی یا نیمه‌عمومی درون سیستمی محدود شده، بیان فهرستی از سایر کاربران که با آن‌ها در ارتباط هستند، مشاهده و گذر از فهرست کسانی‌که با آن‌ها در ارتباط است و سایرین را می‌دهد.»[۴۰]

شبکه اجتماعی سایت یا مجموعه سایتی است برای کاربرانی که دوست دارند علایق، افکارو فعالیت‌های خودشان را با دیگران به اشتراک بگذارند.

در واقع، شبکه‌های اجتماعی شامل ویکی‌ها، وبلاگ‌ها، خبرخوان‌ها[۴۱] و سایر

---

31. myLife
32. myYearbook
33. Badoo

۳٤. برگرفته از سایت:

http://webcache.googleusercontent.com/search?q=cache:http://www.ebizmba.com/articles/social-networking-websites.-

35. Network- Réseau

۳٦. سینکلر، فرهنگ اصطلاحات کامپیوتر و *IT*، ص ٤۹۸.

37. Social
38. Collée, *Ibid*, p. 11.
39. Social Networking Site
40. Boyd & Ellison, "Social network sites: Definition, history, and scholarship", p. 1.
41. RSS (Rich Site Summary)

ابزارهای web 2.0،[۴۲] مجموعه سرویس‌هایی هستند که کارشان به اشتراک‌گذاری محتوا میان کاربران است؛ این محتوا می‌تواند متن، پیوند،[۴۳] عکس، فیلم و یا فایل باشد. کار برخی از این شبکه‌ها مثل یوتیوب،[۴۴] صرفاً اشتراک‌گذاری فیلم و برخی مثل فلیکر اشتراک‌گذاری عکس است؛ برخی مثل ویکی‌پدیا،[۴۵] به صورت مشارکتی متن و محتوا تولید می‌کنند؛ برخی نیز مانند اورکات یا فیس‌بوک، صرفاً برای ارتباطات دوستانه و شبکه سازی میان دوستان کاربرد دارند. از این‌رو،اطلاق شبکه اجتماعی به یک سایت اشتباه است.[۴۶]

بند دوم: انواع شبکه‌های اجتماعی

الف) به لحاظ موضوع

شبکه‌های اجتماعی مجازی دارای موضوعات متفاوتی هستند و حسب موضوع، طیف گسترده‌ای از امکانات را در اختیار کاربران خود قرار میدهند.

برخی شبکه‌های اجتماعی مجازی مثل *لینکداین*[۴۷]، *رایز*[۴۸] و *ویادئو*[۴۹] جنبه شغلی و حرفه‌ای دارند، بدین معنا که این امکان را فراهم می‌کنند تا افراد سوابق و تجارب حرفه‌ای خود را در دسترس قرار دهند تا از این طریق کارفرمایان با ایشان آشنا شوند و از آن‌ها دعوت به همکاری نمایند.[۵۰]

در مقابل، برخی دیگر از شبکه‌ها،غیر حرفه‌ای یا تفنّنی هستند و جنبه سرگرمی دارند، همچون *Spotsvite* که به ورزش، *CarDomain* که به اتومبیل‌ها، *Catster* که به گربه‌ها و *Dogster* که به سگ‌ها می‌پردازند.

در تقسیم‌بندی دیگر می‌توان گفت که به موازات شبکه‌های اجتماعی مجازی عمومی[۵۱] همچون *فیس‌بوک*، *مای‌اسپیس*، *اورکات*، *های‌فایو*، *ببو*، *تگد*، *فرندزتر*، *بلک پلنت* و *بادو*، شبکه‌های اجتماعی تخصصی[۵۲] هر کدام با اهدافی مجزا نیز گسترش

---

۴۲. به نقل از: www.weblognews.ir/1389/02/04.

43. Link
44. YouTube
45. Wikipedia

۴۶. به نقل از: http://socialmedia.ir/?cat=3

47. LinkedIn
48. Ryze
49. Viadéo
50. Balagué & Fayon, "À quoi sert un réseau social?", p. 50.
51. Des réseaux sociaux généralistes
52. Réseaux sociaux spécialisés

یافته‌اند؛ از جمله *MyNASA* به موضوعات هوافضا،*Fotolog* به عکاسی،weread به کتاب، *Flixster* به فیلم‌های سینمایی،*Last.fm* و *Buzznet* به موسیقی، *Flickr* به عکس، *travbuddy* به مسافرت، *Reunion* به دوستان قدیمی و خانواده،*classmates.com* و *graduates.com* به همکلاسی‌ها و فارغ‌التحصیلان اختصاص یافته‌اند.

در فرانسه نیز شبکه *کامپوس*[۵۳] برای دانش آموزان، شبکه *پوپلد*[۵۴] برای هم‌محلی‌ها، شبکه *بوزیمو*[۵۵] برای معاملات مسکن و شبکه‌*مون تریپ*[۵۶] برای مسافرت وجود دارد.[۵۷]

در این میان، شبکه‌ای همانند *اسمال ورلد*[۵۸] خصوصی محسوب می‌شود، یعنی تنها در صورتی که کاربر دیگری شما را دعوت به عضویت کند قادر به عضویت در آن خواهید بود. این شبکه، اختصاصی‌ترین شبکه اجتماعی تنها با ۱۳۰۰۰۰ عضو است که هدف آن تسهیل زندگی اجتماعی برای نخبگان و متفکران اقتصادی است.[۵۹] شبکه‌خصوصی دیگر، سایت *تاپ‌کام* است که تنها ۲۰۰ فرد ثروتمند جهان می‌توانند به عضویت آن درآیند.[۶۰]

ب) به لحاظ روند عضویت

روند عضویت در شبکه‌های اجتماعی اغلب یکسان است؛ برای مثال، در فیس‌بوک متقاضی عضویت در ابتدا باید نام و نام خانوادگی، آدرس ایمیل، رمز اینترنتی، جنسیت و سالروز تولد خود را وارد نماید که غیر از نام بقیه این اطلاعات را می‌تواند برای دیگران غیر قابل مشاهده سازد. پس از انتخاب گزینه ثبت نام،[۶۱] ایمیل تأییدی به ایمیل فرد ارسال می‌شود که با کلیک بر روی لینک موجود، فرد بر قصد خود مبنی بر داشتن حساب[۶۲] صحه می‌گذارد. با کلیک بر روی لینک تأیید[۶۳] کاربر چهار مرحله پیش‌رو دارد:

می‌تواند تقاضای دوستی با فردی دیگر را تأیید کند یا از پذیرش آن امتناع ورزد. (از این گزینه می‌توان به سرعت گذشت)[۶۴].

---

53. Campus
54. Peuplade
55. Buzzimmo
56. Montrip
57. Balagué & Fayon, *op. cit.*, p. 36.
58. SmallWorld
59. Coumet, "Donnees Personnelles & Reseaux Sociaux", p. 4.

۶۰. برای مطالعه بیشتر، نک: http://www.tabnak.ir/fa/news/222314.

61. Sign up
62. Account
63. Confirmation link
64. Skip

۱- از کاربر خواسته می‌شود دوستانی پیدا کند. (از این گزینه نیز می‌توان به سرعت گذشت).

۲- از کاربر تقاضا می‌شود صفحه یا پروفایل خود را تکمیل کند و اطلاعاتی در مورد محل تحصیل و کار خود ارائه دهد. در صورت تمایل، این مرحله نیز قابل عبور است.

۳- در این مرحله از کاربر خواسته می‌شود موقعیت جغرافیایی خود (شهر و کشور) را مشخص کند.

با تکمیل این مراحل، کاربر دارای صفحه یا پروفایل فیس‌بوک است. در این صفحه گزینه‌های دیگری هم وجود دارد همچون: «افرادی که ممکن است بشناسید»[۶۵]، «افرادی را که می‌شناسید پیدا کنید»[۶۶]. با کلیک بر گزینه «نمایش و تنظیم پروفایل خود»[۶۷] تمامی اطلاعات وارد شده از قبیل: اطلاعات پایه (جنسیت و تاریخ تولد، کاربر مختار است این گزینه را غیرقابل‌مشاهده سازد)؛ محل تولد، وضعیت تأهل، نظرات سیاسی و مذهبی، اطلاعات خصوصی (علایق و سرگرمی‌ها، موسیقی و برنامه‌های تلویزیونی و فیلم‌های سینمایی و کتب مورد علاقه)، اطلاعاتی برای برقراری ارتباط (آدرس پست الکترونیکی، شماره تلفن همراه، آدرس وبلاگ)، اطلاعات مربوط به کار و تحصیل (دانشگاه، مدرک) نمایش داده می‌شود؛ با این توضیح که تغییر و اصلاح آن از طریق تنظیمات حریم خصوصی[۶۸] امکان‌پذیر است.[۶۹]

ج) به لحاظ کاربران

افراد با انگیزه‌های مختلفی به سمت شبکه‌های اجتماعی مجازی کشیده می‌شوند. بر این اساس، برخی نویسندگان، کاربران این شبکه‌ها را به شش دسته تقسیم کرده‌اند: پدیدآورندگان[۷۰] (کسانی‌که بلاگ یا صفحهٔ اینترنتی[۷۱] راه‌اندازی می‌کنند، ویدئو، موسیقی، مقاله و نوشته‌های خود را منتشر می‌کنند)، منتقدان[۷۲] (کسانی‌که بلاگ دیگران را تفسیر می‌کنند، در بلاگ دیگران مقاله‌ای را منتشر می‌کنند)، جمع‌آوری‌کنندگان[۷۳]

65. People you may know
66. Find people you know
67. View and edit your profile
68. Privacy settings
69. Barrigar, *Social Network Site Privacy (A Comparative analysis of 6 sites)*, pp. 8-9.
70. Creators
71. Web page
72. Critics
73. Collectors

(کسانی‌که در رای‌گیری‌های آنلاین شرکت می‌کنند، بر عکس دیگران برچسب[۷۴] می‌زنند)، ملحق‌شوندگان[۷۵] (دارندگان پروفایل در شبکه‌های اجتماعی مجازی)، ناظران و مستمعان[۷۶] (خوانندگان بلاگ‌ها، بینندگان ویدئوها، شنوندگان موسیقی)، کاربران منفعل[۷۷] (افرادی غیر از موارد مذکور).

بخش دوم: تهدیدها علیه حریم خصوصی در شبکه‌های اجتماعی مجازی و نحوه حمایت از آن‌ها

بند اول: تهدیدها علیه حریم خصوصی در شبکه‌های اجتماعی مجازی

با گسترش استفاده از شبکه‌های اجتماعی مجازی مسأله حریم خصوصی به یکی از مهم‌ترین دغدغه‌های این حوزه تبدیل شده است. حریم خصوصی قلمروی از زندگی هر فرد است که آن فرد نوعاً عرفاً یا با اعلان قبلی، انتظار دارد دیگران بدون رضایت وی به اطلاعات راجع به آن قلمرو دسترسی نداشته باشند یا به آن قلمرو وارد نشوند یا به آن قلمرو نگاه یا نظارت نکنند و یا به هر صورت دیگری وی را در آن قلمرو مورد تعرض قرار ندهند.[۷۸] شبکه‌های اجتماعی به شیوه‌های مختلفی، حریم خصوصی افراد را در معرض تهدید قرار داده‌اند: گاهی خود آن‌ها از اطلاعات خصوصی کاربران سوءاستفاده می‌کنند و گاهی زمینه و بستر لازم برای سوءاستفاده از سوی دیگران را فراهم می‌سازند. همچنین یکی از مجاری مزاحمت‌های مجازی هستند که از مصادیق نقض حریم خصوصی است.

الف)تهدیدهای موجود علیه داده‌های شخصی کاربران

داده شخصی عبارت است از هرگونه اطلاعات راجع به یک شخص با هویت مشخص یا قابل شناسایی؛ شخص قابل شناسایی کسی است که مستقیم یا غیرمستقیم، به‌ویژه از طریق مراجعه به یک شماره تشخیص هویت یا یک یا چند عامل خاص درباره هویت جسمانی، روانی، ذهنی، اقتصادی، فرهنگی یا اجتماعی قابل شناسایی است.[۷۹]

74. Tags
75. Joiners
76. Spectators
77. Inactives

۷۸. انصاری، آزادی اطلاعات، ۲۳۲.

۷۹. انصاری، حقوق حریم خصوصی، ۲٦٦.

از آنجا که امروزه افراد بیش‌ازپیش از فناوری‌های دیجیتالی همچون پست الکترونیک، اتاق‌های گفت‌وگو و شبکه‌ها استفاده می‌کنند، با استفاده از این خدمات آنلاین، بخش وسیعی از اطلاعات خود را افشا می‌سازند، سیستم‌های اطلاعاتی و ارتباطی هم بسیار پیچیده و گمراه کننده هستند و اغلب کاربران نمی‌دانند چه نوع از داده‌هایشان تا چه میزان و تا چه مدت ذخیره و نگهداری می‌شود.

۱. از سوی خود شبکه‌اجتماعی

تهدیدها علیه داده‌های شخصی کاربران، گاه از ناحیه خود شبکه‌ها، به واسطه *برنامه‌های* موجود یا همان اپلیکیشن‌ها[۸۰] صورت می‌گیرد. برنامه‌های متفاوت موجود در شبکه‌های اجتماعی مجازی،از مهم‌ترین ابزارهایی هستند که به واسطه آن‌ها دسترسی به داده‌های اشخاص آسان می‌گردد. این برنامه‌ها برای کاربران بسیار جذاب هستند چراکه آن‌ها را در برقراری هرچه بیشتر ارتباطات کمک می‌کنند. هنگام عضویت در شبکه‌ها، برخی برنامه‌ها به طور خودکار به کاربر پیشنهاد می‌شوند؛ برخی برنامه‌ها این امکان را فراهم می‌کنند تا کاربر، تصاویر خود را بر صفحه‌اش قرار دهد، فهرستی از آهنگ‌های مورد علاقه خود را تهیه کرده و هنگامی که آنلاین است گوش دهد.این برنامه‌ها حسب نوع و اهداف شبکه‌ها متفاوت هستند.

شبکه‌ای همچون فیس‌بوک اطلاعات کاربران را در پایگاه داده‌های خود[۸۱] نگهداری می‌کند، حتی اگر کاربر پروفایل و اطلاعاتش را پاک کند کماکان این اطلاعات در پایگاه داده‌ها باقی می‌ماند؛ درواقع به کاربر این حق داده نمی‌شود که فراموش شود.البته اتحادیه اروپا از حق بر محو شدن[۸۲] که در حقوق فرانسه حق بر فراموشی[۸۳] نامیده می‌شود قویاً حمایت می‌کند و کمیسیون اروپا در حال مذاکره با فیس‌بوک است تا حق بر فراموشی را برای کاربرانی که اطلاعاتشان را پاک می‌کنند اعمال کند و به کاربران به روشنی توضیح دهد که چه کسانی داده‌های ایشان را جمع‌آوری کرده، مورد استفاده قرار می‌دهند و این داده‌ها تا چه مدت نگهداری می‌شوند.[۸۴]

۲. از سوی اشخاص ثالث

تهدید دیگر علیه داده‌های شخصی ممکن است از ناحیه اشخاص ثالث صورت گیرد. منظور از اشخاص ثالث، هم اشخاص حقیقی ثالث و هم اشخاصی هستند که

80. Applications
81. Database
82. Right to disappear
83. le droit à l'oubli
84. Tsaoussi, *op. cit.*, 8.

تهیه‌کننده و فراهم‌آورنده برنامه‌ها هستند و هنگامی که کاربر برنامه خاصی را به فهرست خود اضافه کند به داده‌های او دسترسی پیدا می‌کند. علاوه بر برنامه‌هایی که در شبکه‌های اجتماعی مجازی وجود دارند و به کاربر پیشنهاد می‌شوند، برنامه‌سازان ثالث هم می‌توانند برنامه خاصی را ساخته و روی سایت قرار دهند و تصمیم با کاربر است که در صورت تمایل، برنامه‌ها را دانلود و از آن‌ها استفاده کند. این برنامه‌ها که از سویی، کاربران را سرگرم و از سوی دیگر، صفحات آن‌ها را زیباتر می‌کنند می‌توانند در قالب بازی‌ها، پرسش و آزمون، نظرسنجی و سایر فرم‌ها ارائه شوند. کاربر می‌تواند به صورت آنلاین با دوستانش بازی کند، آهنگی را که یکی از همکارانش در سایت قرار داده گوش کند و به وسیله‌برخی برنامه‌ها با افراد جدید آشنا شود. این برنامه‌ها پایانی ندارند و تعدادشان روزبه روز در حال گسترش است. اخیراً برخی شرکت‌ها با هدف تهیه چنین برنامه‌هایی ایجاد شده‌اند که نمونه مهم این شرکت‌ها شرکت حقوقی آمریکایی *لیوینگ سوشال*[85] است که برنامه‌های آن در شبکه‌های فیس‌بوک و توئیترشهرت جهانی یافته است.

این برنامه‌ها یکی از علل گسترش شبکه‌های اجتماعی مجازی هستند. برای مثال می‌توان از شبکه مای‌اسپیس نام برد که تمرکز آن بر موسیقی است. هر کاربر می‌تواند آهنگی را که دوست دارد یا حتی آهنگی را که خود ساخته در این شبکه منتشر کند. بدین ترتیب، مای‌اسپیس به شبکه‌ای تبدیل شده است که به شکوفایی استعداد افراد در زمینه موسیقی کمک می‌کند و این فرصت را برای هنرمندان جوانی که قادر به ثبت و ضبط و پخش آثار خود نیستند فراهم می‌سازد تا آن‌ها را عرضه کنند.

برای حضور در این عرصه، لزوماً نیازی به ثبت نام در شبکه‌های اجتماعی مجازی نیست. می‌توان گروه‌هایی تشکیل داد تا کاربران به آن‌ها ملحق شوند. برای مثال، طرفداران یک هنرمند از این شیوه برای حمایت از وی استفاده می‌کنند. حدود ۵۰۰ گروه در فیس بوک به گروه *بیتلز*[86] اختصاص یافته است و بسیاری گروه‌ها در سایر مسائل فرهنگی، موسیقی، سینما و ادبیات هم وجود دارند.

این برنامه‌ها امکان جمع‌آوری داده‌های اشخاص، داده‌هایی راجع به علایق، شخصیت، تمایلات و نیازهای اشخاص را فراهم می‌آورند. برای مثال برنامه *لیوینگ‌سوشال* که بیشترین کارکرد را در فیس‌بوک داشته است، از کاربران فیس‌بوک

85. Living social
86. Beatles

می‌خواهد تا پنج کتاب، فیلم، آهنگ و شخصیت مورد علاقه خود را انتخاب و با دوستان و سایر افراد مرتبط با خود[۸۷] به اشتراک گذارند. هدف این برنامه شناسایی علایق کاربران است. برنامه‌دیگری که مورد توجه کاربران بوده است برنامه زوسک است که نوعی آژانس ازدواج می‌باشد و این امکان را فراهم می‌آورد تا شخص با سایر کاربرانی که علایق و محلسکونت مشابه دارند آشنا شود.

میزان افشای داده‌های شخصی که برای مشارکت در چنین برنامه‌ای صورت می‌گیرد، بسیار زیاد است. گفته شده که ماهانه از برنامه *لیوینگ‌سوشال*، حدود ۳۱/۷۷۲/۸۹۱ کاربر و از برنامه‌زوسک حدود ۸/۵٤۱/٤٤۳ کاربر استفاده می‌کنند. در عمل، داده‌هایی که هنگام ثبت نام و عضویت در شبکه از کاربر خواسته نمی‌شود و یا داده‌هایی که کاربر خود تمایلی به افشاء آن‌ها ندارد، از این طریق و تحت پوشش چنین برنامه‌هایی فاش می‌شود.

در واقع، برنامه‌سازان می‌توانند بدون موافقت صریح و رضایت کاربر، از این طریق، نه تنها اطلاعات خود کاربر بلکه حتی اطلاعات دوستان کاربر را جمع‌آوری کنند. کاربر با الحاق به این برنامه‌ها بدون اینکه وکالت یا اختیاری از دیگری داشته باشد این امکان را برای برنامه‌سازان فراهم می‌کند که اطلاعات اشخاص دیگر را هم پردازش کنند؛ درعمل، چون کاربر قادر به اعلام رضایت یا عدم رضایت خود نیست، اطلاعاتی که از این طریق به وسیله برنامه‌سازان جمع‌آوری می‌شود، بدون رضایت صاحبان آن‌ها بوده و غیرقانونی است.

بنابراین، در ظاهر، این برنامه‌ها جنبه سرگرم کنندگی و تزئینی دارند اما در حقیقت، از طریق آن‌ها، داده‌های اشخاص جمع‌آوری می‌شود و ممکن است به فروش برسد. این برنامه‌سازان مستقل از شبکه‌ها هستند و اغلب محل فعالیت و استقرارشان کشوری غیر از کشور متبوع کاربر است، در صورتی‌که کاربر متوجه سوءنیت برنامه‌سازان شود می‌تواند از آن‌ها شکایت کند. اما مطابق مقررات شبکه‌ها، هنگام الحاق به این برنامه‌ها صراحتاً مقرر شده است که این برنامه‌ها نوعی توافق میان کاربر و برنامه‌ساز است و شبکه اجتماعی در این زمینه از هرگونه مسؤولیت مبری است. شرکت‌هایی که با هدف سوءاستفاده، چنین برنامه‌هایی را تهیه کرده‌اند برای فرار از مسؤولیت، یا اطلاعات خود را در اختیار شبکه‌ها قرار نمی‌دهند یا اطلاعات قدیمی و غلط ارائه می‌دهند؛ بنابراین عملاً دسترسی به آن‌ها و شناسایی آن‌ها دشوار است.

87. Contacts

علاوه بر این، اثبات سوءنیت برنامه‌ساز از سوی کاربر دشوار است و وی حتی اگر متوجه جمع‌آوری غیرمجاز اطلاعات شخصی خود شده باشد باز به نظر می‌رسد برای جلوگیری از استفاده از آن‌ها دیر شده باشد چراکه برنامه‌ساز ممکن است اطلاعات را به شرکت‌های تبلیغاتی یا سایر شرکت‌ها فروخته باشد که غالباً شناسایی موارد اخیر غیرممکن است. در نتیجه عملاً خسارت جبران نشدنی است.[۸۸]

۳. از سوی بدافزارها

بدافزارها، تهدیدی دیگر علیه داده‌های شخصی کاربران هستند. استفاده از برخی بدافزارها برای نفوذ در رایانه‌های شخصی و جمع‌آوری اطلاعات شخصی افراد تهدید جدیعلیه حریم خصوصی ایجاد کرده‌است. بدافزار، ترجمه‌ای از واژه malware، از ادغام دو واژه malicious و software به وجود آمده است. منظور از بدافزارها، نرم‌افزارهایی هستند که به منظور تکثیر و تخریب اطلاعات در برنامه نفوذ می‌کنند. این ویروس‌ها با توجه به اهداف مدنظر سازندگان خود گوناگون هستند برای مثال در سال ۲۰۰۶ تعداد ویروس‌های متفاوت ۲۰۰۰۰۰ تخمین زده شد در حالی که سال ۱۹۸۹ تعداد آن‌ها تنها ۱۸ مورد بوده است. پس این ارقام همچنان رو به افزایش است.

بدافزارها انواع مختلف دارند که در این میان، جاسوس‌افزارها و تبلیغ‌افزارها تهدیدکننده حریم خصوصی هستند.

جاسوس‌افزارها[۸۹] جدیدترین تهدیدها همزمان با همگانی شدن اینترنت و خصوصاً شبکه‌های اجتماعی مجازی محسوب می‌شوند. مجرمین، اطلاعاتی را جمع‌آوری می‌کنند که بتوانند آن را به مبلغ خوبی بفروشند. برای مثال برنامه‌ای به نام *لاور اسپای*[۹۰] وجود دارد که با ۸۹ دلار هدایایی را برای نامزد[۹۱] فرد می‌فرستد، در واقع این برنامه، نرم‌افزاری برای جاسوسی است بدین صورت که مجرمین از طریق آن به اسرار و رازهای خصوصی افراد که در رایانه‌های شخصی نگهداری می‌شوند دسترسی پیدا می‌کنند.

نمونه دیگر جاسوس‌افزارها، برنامهٔ کی لاگر[۹۲] است که به صورت محرمانه اطلاعات وارد شده بر صفحه کلید کامپیوتری که بر روی آن نصب شده را ضبط کرده و سپس آن را به طور مخفیانه برای مالک برنامه می‌فرستد. این برنامه روش کارکردی

88. Coumet, *op. cit.*, 47-51.
89. Spyware
90. Loverspy
91. Fiancée
92. Keylogger

هوشمندانه دارد بدین معنا که تمامی داده‌ها را ضبط نمی‌کند بلکه داده‌های مفید را ثبت می‌کند تا بین سایر داده‌ها گم و محو نشوند.

اخیراً توئیتر قربانی حمله یکی از جاسوس‌افزارها شده بود. فردی با عضویت در این شبکه، ازطریق یک پیوند، ویدئوهای پورنوگرافیک منتشر می‌کرد. هنگامی که کاربر دیگری روی این پیوندها کلیک می‌کرد، پنجره دانلود اتوماتیک باز شده و وانمود می‌شد که برنامه *اداب فلش*[۹۳] (که برای مشاهده ویدئوها ضروری است) در حال به‌روزشدن است؛ بدین ترتیب روی کامپیوتر کاربر پوشه جدیدی به نام *اداب فلش* ظاهر می‌شد در حالی‌که برنامه‌ای برای ذخیره داده‌های فرد و ارسال آن به حساب فرد خاطی ایجاد شده بود. نهایتاً، توئیتر پس از اطلاع از این موضوع حساب آن کاربر را مسدود کرد.

تبلیغ‌افزارها[۹۴] نیز نوع خاصی از جاسوس‌افزارها هستند کهداده‌های شخصی را به منظور انتقال این داده‌ها به شرکت‌های مخصوص بازاریابی آنلاین، جمع‌آوری می‌کنند، برای مثال برنامه*کازا*[۹۵] که در مقابل جمع‌آوری داده، خدمات رایگان تبلیغاتی ارائه می‌دهد.

نهایتاً، *اسپم‌ها*[۹۶] (بسته‌های ارسالی به پست الکترونیک افراد که *هرزنامه* ترجمه شده است) به عنوان تهدید دیگر علیه داده‌های شخصی کاربران محسوب می‌شوند. در خصوص اسپم‌ها، نقش شبکه‌های اجتماعی مجازی بدین گونه است که شناسایی پست الکترونیک افراد و به دنبال آن ارسال اسپم‌ها،ممکن است از طریق شبکه‌ها صورت گیرد. این پیغام‌های ناخواسته به پست الکترونیک، حتی اگر خطر قربانی شدن در یک جرم را به همراه نداشته باشند، مسلماً بسیار ناخوشایند هستند.

علی‌رغم آنچه گفته شد، به نظر می‌رسد که مهم‌ترین تهدیدها «عوامل انسانی» هستند، منظور عدم شناخت و درک کافی کاربران از برنامه‌ها به علت پیچیدگی آن‌هاست. با گسترش برنامه‌ها، طبیعی است که تعداد اشتباهات برنامه‌نویسان هم افزایش می‌یابد و طبیعتاً تهدیدها علیه حریم خصوصی کاربران افزایش می‌یابد.[۹۷]

ب) مزاحمت‌های مجازی و شبکه‌های اجتماعی مجازی

تقریباً همه افراد در زندگی روزمره خود با آزار و اذیت‌مواجه شده‌اند. cyber bullying

93. Adobe Flash
94. Adware
95. Kazaa
96. Spam
97. Coumet, *op. cit.*, 51-53.

یک اصطلاح ترکیبی است؛ bully به شخص مغرور، ظالم و قلدر خصوصاً در مقابل افراد ضعیف و کوچک‌تر گفته می‌شود که از ترکیب آن با واژه cyber، ترکیب cyber bullying شکل می‌گیرد.بنابراین، مزاحمت مجازی عبارت است از: «به کارگیری فناوری اطلاعات و ارتباطات در انجام فعالیت‌های عمدی، مکرر و دشمنانه از سوی فرد یا گروهی از افراد به قصد آزار دیگران.» این اشخاص با استفاده از پست‌های الکترونیکی، پیام‌های مکرر، اتاق‌های گفت‌وگو و ارسال پیام به تلفن همراه قربانیان خود موجب ناراحتی آن‌ها می‌شوند.[۹۸] علی‌رغم شباهت‌هایی که مزاحمت‌های مجازی با مزاحم‌های سنتی دارد، اما بسیار ویرانگرتر از مزاحمت‌های سنتی می‌دانند. بدین‌علت که قربانیان اغلب نمی‌دانند چه‌کسی ایشان را آزار می‌دهد، ممکن است از علت این آزار هم آگاهی نداشته باشند. مزاحم[۹۹] ممکن است هویت خود را در رایانه شخصی، تلفن همراه یا پست الکترونیک پنهان کرده و به صورت ناشناس به آزار و اذیت بپردازد.[۱۰۰] پس از لحاظ روانی نیز قربانی صدمه بیشتری می‌بیند چرا که اغلب کسی را که او را آزار می‌دهد نمی‌شناسد، در نتیجه، احساس ضعف و ناتوانی می‌کند.

پرونده *مگان میر*[۱۰۱] ۱۳ ساله اهل میسوری[۱۰۲]، مثالی از مزاحمت‌های مجازی است که به دنبال شوخی و مزاحمتی بچه‌گانه در مای‌اسپیس دست به خودکشی زد. او از طریق مای‌اسپیس با فردی به نام *جاش*[۱۰۳] آشنا شد، پس از ماه‌ها ارتباط اینترنتی دوستانه، پیام‌های جاش یکباره قطع و آخرین پیام او تحت عنوان «بی‌شک دنیا بی‌تو مکان بهتری است» سبب شد تا ۲۰ دقیقه بعد مگان خود را حلق‌آویز کند. شش هفته پس از این اتفاق، والدین مگان متوجه شدند که جاش، مادر یکی از دوستان مگان است که با ساخت شخصیتی جعلی در شبکه اجتماعی مای‌اسپیس در پی آن بوده است تا نظر مگان در خصوص دخترش را جویا شود.[۱۰۴]

با گسترش استفاده از فناوری‌های نو و تجهیزاتی که از طریق روش‌های سنتی قابل کنترل نیستند، اصطلاح دیگری تحت عنوان cyber stalking جایگزین روش‌های قدیمی آزار و اذیت شده است. این اصطلاح این‌گونه تعریف شده است: «استفاده از ارتباطات

98. Aldinger, *op. cit.*, 17.
99. Cyberbully

۱۰۰. برای مطالعه بیشتر، نک:

http://www.cyberbullying.us/Cyberbullying_Identification_Prevention_Response_Fact_Sheet.pdf.

101. Megan Meier
102. Missouri
103. Josh
104. Aldinger, *op. cit.*, 4.

و روش‌های الکترونیکی برای آزار دیگران». Stalking به معنای رفتاری آزاردهنده و تهدیدآمیز و مکرر نسبت به یک شخص است، همچون دنبال کردن و تعقیب فرد، حضور در منزل یا محل کار وی، تماس‌های تلفنی مزاحمت آمیز، به جا گذاشتن نوشته‌ها و پیغام‌های تهدیدآمیز ...»

تحقق این عمل مستلزم آن است که تهدیدی واقعی، معتبر و مؤثر اتفاق افتاده باشد و این مشکل‌ساز است چرا که اغلب چنین مزاحمانی برای قربانی ناشناس هستند و عموماً در فاصله‌ای دور از قربانی قرار دارند به همین علت ممکن است تهدید مؤثر شناخته نشود. بنابراین بهتر است «رفتارهایی که شخص را در حالت ترس منطقی از مرگ و ضرب و شتم» قرار می‌دهند، جرم انگاری شوند.[۱۰۵]

در خصوص شبکه‌های اجتماعی مجازی، مجرمین ازاین شبکه‌ها برای تهدید و ارعاب قربانیان خود استفاده می‌کنند و همان‌طور که گفته شد از آنجاکه اغلب ناشناس و غیرقابل دسترس برای کاربران هستند اعمال مقررات در این حوزه با سختی روبه‌رو می‌شود.

مسأله دیگر حضور مجرمین یا افرادی که محکومیت خود را طی کرده‌اند یا در حال طی محکومیت خود هستند در فیس‌بوک است. برای مثال برخی زندانیان در بریتانیا متهم شده‌اند که از فیس‌بوک برای آزار و اذیت قربانی‌هایشان استفاده می‌کردند، خانواده قربانیان هم از فیس‌بوک و سایر شبکه‌های اجتماعی خواستند که در این خصوص اقدامی کرده و مسؤولیت پذیر باشند؛ فیس بوک هم در پاسخ،پروفایل بیش از ۳۰ تن از این محکومین را که از زندان به وسیله فیس‌بوک قربانی‌های خود را مورد آزار و اذیت قرار می‌دادند، مسدود کرد.[۱۰۶]

بند دوم: شیوه حمایت از حریم خصوصی در شبکه‌های اجتماعی مجازی

برای مقابله با تهدیدهای موجود علیه حریم خصوصی در شبکه‌های اجتماعی مجازی سه شیوه مهم مورد توجه واقع شده است: تسری حمایت‌های موجود از داده‌های شخصی به حمایت از حریم خصوصی در فضای مجازی، تصویب اسناد و مقررات خاص برای حمایت از حریم خصوصی در فضای مجازی و تنظیم سیاست‌های حریم خصوصیِ شبکه‌های اجتماعی مجازی.

105. *Ibid*, 19.
106. Milivejovic, *op. cit.*, 3.

الف) تسری حمایت‌های موجود از داده‌های شخصی به حمایت از حریم خصوصی در فضای مجازی

حق حریم خصوصی بعنوان یکی از مصادیق مهم حقوق بشر شناخته می‌شود و در بسیاری از اسناد بین‌المللی راجع به حقوق بشر نظیر اعلامیه جهانی حقوق بشر (۱۹٤۸)، کنوانسیون اروپایی حمایت از حقوق بشر و آزادی‌های بنیادین (۱۹۵۰)، کنوانسیون آمریکایی حقوق بشر (۱۹٦۹)، میثاق بین‌المللی حقوق مدنی و سیاسی (۱۹٦٦) و اعلامیه اسلامی حقوق بشر (۱۹۹۰) به غیر قابل تعرض بودن آن تصریح شده است.

از سوی دیگر، اهمیت داده‌های شخصی و ارتباط آن‌ها با آزادی، استقلال و کرامت انسانی سبب شده است که در برخی اسناد خارجی، حق افراد در مصون بودن داده‌های شخصی آن‌ها از تعرض‌های غیرقانونی، یکی از حقوق بشر یا اساسی محسوب شود و حمایت‌های جدی از آن به عمل آید. در میان اسناد بین‌المللی همچون «رهنمودهای سازمان همکاری و توسعه اقتصادی (OECD) درباره حمایت از حریم خصوصی و جریان فرامرزی داده‌های شخصی در سال ۱۹۸۰»[۱۰۷]، «دستورالعمل شورای اروپا در حمایت از داده‌های شخصی» تحت عنوان «کنوانسیون حمایت از افراد در برابر پردازش خودکار داده‌های شخصی»[۱۰۸] مصوب ۱۹۸۱، مهم‌ترین سندی است که درباره داده‌های شخصی تصویب شده و الگوی بسیاری از کشورها در تهیه و تصویب مقررات راجع به حمایت از داده قرار گرفته است.[۱۰۹]

پس از آن، «قطعنامه مجمع عمومی سازمان ملل متحد با عنوان رهنمودهایی برای قاعده‌مندسازی فایل‌های رایانه‌ای داده‌های شخصی در سال ۱۹۹۰»[۱۱۰]، «دستورالعمل حمایت از افراد در برابر پردازش داده‌های شخصی و جریان آزاد داده‌ها مصوب شورا و پارلمان اروپا در سال ۱۹۹۵»[۱۱۱]، «منشور حقوق اساسی اتحادیه اوپا در سال ۲۰۰۰»[۱۱۲]، «دستورالعمل راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی

107. OECD Guidelines on the protection of privacy and transborder flows of personal data of 23 september 1980.

108. Convension for the Protection of Individuals with Regard to Automatic Processing of Personlal Data.

۱۰۹. انصاری، حقوق ارتباط جمعی، ۲۰۳.

110. United Nations Guidelines for the regulation of computerised personal data files, adopted by the General Assembly Resolution 45/90 of 14 December 1990.

111. Directive on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.

112. Charter of Fundamental Rights of the European Union of 7 December 2000.

ارتباطات الکترونیکی اتحادیه اروپا در سال ۲۰۰۲»[۱۱۳]، «دستورالعمل نگهداری داده‌های شخصی تولید یا پردازش شده در چارچوب تأمین خدمات ارتباطی الکترونیکی قابل دسترسی برای عموم یا شبکه‌های عمومی ارتباطی و اصلاح دستورالعمل ۲۰۰۲ اتحادیه اروپا در سال ۲۰۰۶»[۱۱۴] و «طرح مشترک پیش‌نویس استانداردهای بین‌المللی حمایت از حریم خصوصی در برابر پردازش داده‌های شخصی در سال ۲۰۰۹»[۱۱۵] در راستای حمایت از داده‌های شخصی به تصویب رسیده اند.

در کنار اسناد مذکور، به اصول حمایت از داده‌های شخصی نیز می‌توان اشاره نمود؛ اصولی که کم و بیش در کشورهای مختلفی که نظام خاصی برای حمایت از داده‌ها طراحی کرده‌اند مورد پذیرش و توجه خاص است. این اصول دربردارنده نکاتی در خصوص جمع‌آوری داده‌های شخصی، استفاده از داده‌های شخصی، به گردش انداختن داده‌های شخصی، جریان فرامرزی داده‌های شخصی و دسترسی به داده‌های شخصی و تصحیح داده‌های نادرست هستند.[۱۱۶]

ب) تصویب اسناد خاص برای حمایت از حریم خصوصی در شبکه‌های اجتماعی مجازی

برای حمایت از حریم خصوصی در شبکه‌های اجتماعی مجازی، اسنادی مرتبط به طور پراکنده تنظیم شده‌اند که نشانگر وقوف جامعه بین‌الملل بر اهمیت این موضوع است. با وجود این، هنوز سند الزم آوری در این خصوص تصویب نشده است و اسناد مذکور عموماً جالت توصیه‌ای و ارشادی دارند. برخی از این اسناد عبارتند از:

– «گزارش و رهنمود درباره حریم خصوصی در شبکه‌های اجتماعی»[۱۱۷]: این گزارش، یادداشتی غیر رسمی است که در چهل‌وسومین نشست کارگروه بین‌المللی راجع به حمایت از داده‌ها در ارتباطات از راه دور، (مارس ۲۰۰۸) در رم ایتالیا صادر شده است. گزارش مذکور، مروری بر شبکه‌های اجتماعی مجازی داشته و به ذکر تهدیدها علیه حریم خصوصی و امنیت افراد می‌پردازد و پیشنهادهایی را به قانونگذاران، تهیه‌کنندگان شبکه‌ها و کاربران ارائه می‌دهد. در نهایت، به سازمان‌های حمایت‌کننده از

113. Directive Concerning Processing of Data and the Protection of Privacy in the Electronic Communication Sector.

114. DIRECTIVE 2006/24/EC 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

115. Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data of 5 November 2009.

۱۱۶. برای مطالعه بیشتر، نک: انصاری، حقوق حریم خصوصی، ۲۸۳–۲۷۰.

117. Report and Guidance on Privacy in Social Network Services.

حقوق مصرف‌کننده و حریم خصوصی توصیه می‌کند تا تدابیری مناسب برای افزایش آگاهی قانونگذاران، تهیه‌کنندگان شبکه‌ها، عامه مردم و به ویژه جوانان در خصوص تهدیدهای موجود علیه حریم خصوصی در صورت استفاده از شبکه‌ها، اتخاذ کنند.

– «پیش‌نویس قطعنامه راجع به حریم خصوصی در شبکه‌های اجتماعی مجازی»[۱۱۸]: این پیش‌نویس به پیشنهاد کمیسیون حمایت از داده‌ها و آزادی اطلاعات ایالت برلین آلمان[۱۱۹] و با همکاری کمیسیون ملی انفورماتیک و آزادی‌های فرانسه[۱۲۰]، کمیسیون فدرال حمایت از داده‌ها و آزادی اطلاعات آلمان[۱۲۱]، کمیسیون حمایت از داده‌های ایتالیا[۱۲۲]، کمیسیون حریم خصوصی نیوزیلند[۱۲۳]، کمیسیون فدرال حمایت از داده و اطلاعات سوئیس[۱۲۴]، در سی‌امین کنفرانس بین‌المللی حمایت از داده‌ها و حریم خصوصی که در اکتبر ۲۰۰۸ در استراسبورگ تهیه گردید. این پیش‌نویس به کاربران توصیه می‌کند که جانب احتیاط را رعایت کنند، به ویژه کودکان و نوجوانان را از قراردادن آدرس محل سکونت و شماره تلفن در پروفایل خود برحذر می‌دارد و از کاربران می‌خواهد که به حریم خصوصی دیگران احترام گذاشته و اطلاعات آن‌ها را، بدون رضایت قبلی، منتشر نسازند. مطابق این پیش‌نویس، تهیه‌کنندگان شبکه‌ها نیز دارای مسؤولیتی خاص در قبال داده‌های شخصی افراد هستند؛ بایستی به قوانین حریم خصوصی کشوری که در محدوده آن اقدام به فعالیت نموده‌اند، احترام بگذارند و با مقامات مربوطه به مشورت بپردازند؛ باید کاربران را از روند پردازش داده‌ها مطلّع سازند، به کاربران اجازه نظارت کافی بر داده‌های خود را بدهند و تمامی تلاش خود را برای ارتقاء سیستم امنیتی حمایت از داده‌های کاربران بکار گیرند.

– «اصول شبکه اجتماعی امن‌تر برای اتحادیه اروپا»[۱۲۵]: این سند که در فوریه ۲۰۰۹ توسط کمیسیون اتحادیه اروپا با همکاری تعدادی از تهیه‌کنندگان شبکه‌های اجتماعی منتشر شده‌است، ضمن ارائه رویکردهایی جهت حمایت از حقوق کاربران، اصولی را مطرح می‌کند که با الگو قراردادن آن‌ها، تهیه‌کنندگان شبکه‌ها موظف خواهند شد که تهدیدات علیه کودکان و نوجوانان را به حداقل برسانند.

118. Draft Resolution on Privacy Protection in Social Network Services.
119. Data Protection and Freedom of Information Commissioner of the State ofBerlin, Germany.
120. Commission Nationale de l'Informatique et des Libertés (CNIL), France.
121. Federal Commissioner for Data Protection and Freedom of Information, Germany.
122. Garante per la protezione dei dati personali, Italy.
123. Privacy Commissioner, New Zealand.
124. Federal Data Protection and Information Commissioner (FDPIC), Switzerland.
125. Safer Social Networking Principles for the EU.

– «توصیه کارگروه ماده ۲۹ راجع به حمایت از داده‌ها درباره شبکه‌های اجتماعی مجازی، مورخ ژوئن ۲۰۰۹»[۱۲۶]: این کارگروه که بر مبنای ماده ۲۹ دستورالعمل ۱۹۹۵ راجع به حمایت از افراد در برابر پردازش داده‌های شخصی و جریان آزاد داده‌ها، تشکیل شده است، سازمان مشورتی مستقلی است که به بررسی مسائل مربوط به حمایت از داده و حریم خصوصی می‌پردازد. مأموریت کارگروه مذکور در ماده ۳۰ دستورالعمل ۱۹۹۵ و ماده ۱۵ دستورالعمل ۲۰۰۲ راجع به پردازش داده‌های شخصی و حمایت از حریم خصوصی ارتباطات الکترونیکی، آمده است و هدف از تشکیل آن، ارائه معیارهایی به تهیه‌کنندگان شبکه‌ها جهت تضمین رعایت حقوق افراد، عنوان شده است.این کارگروه به دنبال طرح روشی است که بر مبنای آن، شبکه‌های اجتماعی توانایی پاسخگویی در برابر مقررات‌گذاری‌های اتحادیه‌اروپا راجع به حمایت از داده‌ها را داشته‌باشند. توصیه‌نامه مذکور، نخست به تعریف شبکه‌های اجتماعی پرداخته، از دستورالعمل‌های راجع به حمایت از داده یاد کرده و موارد مذکور در آن‌ها را قابل اجرا در شبکه‌ها دانسته است و سپس به حقوق کاربران (حق احترام به حریم خصوصی و حق دسترسی به اطلاعات) و تعهدات و وظایف شبکه‌ها اشاره می‌کند. برای مثال، تأکید می‌کند که تهیه‌کنندگان شبکه‌های اجتماعی در قبال پردازش داده‌های شخصی کاربران مسؤول هستند، بایستی کاربران را از شیوه جمع‌آوری و پردازش داده‌ها آگاه سازند و به آن‌ها هشدار دهند که از در دسترس قراردادن اطلاعات دیگران به ویژه تصاویر آن‌ها خودداری کنند. مطابق این توصیه‌نامه، شبکه‌ها باید تنظیمات پیش‌فرض خود را با درنظرگیری حق بر حریم خصوصی ارائه دهند وتدابیر فنی لازم را برای حمایت از حریم خصوصی افراد اتخاذ کنند.

– «منشور حریم خصوصی در دنیای دیجیتال»[۱۲۷]: این منشور در چهل‌وهفتمین نشست کارگروه بین‌المللی راجع به حمایت از داده‌ها در ارتباطات از راه دور، مورخ آوریل ۲۰۱۰ در گرانادای اسپانیا تنظیم شده است و دربردارنده توصیه‌هایی به کاربران، ارائه‌دهندگان خدمات و مقامات عمومی برای حفاظت از حریم خصوصیو امنیت افراد است.این منشور به کاربران یادآوری می‌کند که حذف اطلاعات از اینترنت، دشوارتر از انتشار آن‌هاست؛ اخذ رضایت پیش از هرگونه انتشار اطلاعات راجع به دیگری را اجباری می‌داند؛ برقراری ارتباطات مجازی خصوصی، بدون هرگونه مداخله و نظارت

126. Avis 5/2009 sur les réseaux sociaux en ligne, Groupe de Travail «Article 29» sur la Protection des Donnees.

127. The Granada Charter of Privacy in a Digital World, Granada (Spain).

و آگاهی از روند پردازش داده‌های شخصی را حقی اساسی برای کاربران می‌داند. از سوی دیگر، تهیه‌کنندگان را به ایجاد رهنمودهایی برای کاربران، تلاش جهت بهبود کیفیت فنی و افزایش آگاهی کاربران نسبت به تهدیدهای موجود علیه حریم خصوصی، دعوت می‌کند. در نهایت، مقامات عمومی را از هرگونه مشاهده، رهگیری و نظارت بر ارتباطاتافراد مگربرای اجرای قانون، بر اساس مبنای خاص قانونی، منع می‌کند. آن‌ها را ملزم به تضمین دسترسی تمامی افراد با سطوح علمی متفاوت، ایجاد امکانات جهت مشارکت کامل در ارتباطات دیجیتال و ارائه راه‌حل‌های مؤثر در اجرای حقوق کاربر و حق بر حریم نخصوصی و حمایت از داده‌ها می‌نماید.

ج) با توسل به خودتنظیمی

همان‌گونه که اشاره شد، شبکه‌ها بدین جهت مورد انتقاد قرار گرفته‌اند که دسترسی به اطلاعات اشخاص و به دنبال آن نقض حریم خصوصی را تسهیل کرده‌اند. به همین منظور، برای پاسخ به تهدیدها، شبکه‌ها سیاست‌های حریم خصوصی[۱۲۸] خاصی را اتخاذ کرده‌اند.

سیاست‌های حریم خصوصی عموماً دربردارنده موارد زیر است: کدام‌یک از داده‌های شخصی جمع‌آوری می‌شوند؛ داده‌های شخصی چگونه ممکن است مورد استفاده قرار گیرند؛ داده‌های شخصی ممکن است برای چه کسانی افشا شوند؛ تدابیر امنیتی برای حمایت از داده‌های شخصی کدامند و غیره.

شبکه‌ها مدعی‌اند که به واسطه تنظیمات حریم خصوصی از حریم خصوصی افراد حمایت می‌کنند. برای مثال، فیس‌بوک مکرراً سیاست حریم خصوصی خود را بعلت نگرانی‌ها نسبت به نقض حریم خصوصی بازبینی کرده است. بیانیه حقوق و مسؤولیت‌ها[۱۲۹]بر روابط فیس‌بوک با افراد و کاربران آن حاکم است. با عضویت در فیس‌بوک، فرض براینست که کاربر موافق بیانیه مذکور بوده و کلیه حقوق و مسؤولیت‌های ناشی از عضویت را پذیرفته است. در این بیانیه، فیس‌بوک اعلام می‌دارد که برای حریم خصوصی اشخاص اهمیت زیادی قائل است، به همین منظور، با طراحی سیاست استفاده از داده‌ها[۱۳۰] مشخص می‌سازد که کاربران چگونه می‌توانند از این شبکه برای برقراری ارتباط با سایرین استفاده کنند و این شبکه چگونه می‌تواند اطلاعات

128. Privacy Policy
129. Statement of Rights and Responsibilities
130. Data Use Policy

اشخاص را جمع‌آوری و استفاده کند. فیس‌بوک در سیاست استفاده از داده‌های خود صراحتاً اعلام کرده است که اطلاعات کاربران را بدون رضایت ایشان در اختیار آگهی‌دهندگان قرار نمی‌دهد.[۱۳۱] منتها باید دانست که رضایتی حریم خصوصی را منتفی می‌سازد که آگاهانه باشد یعنی کاربر نسبت به مسأله حریم خصوصی مطلع باشد. همچنین صرف انتشار اطلاعات در شبکه به‌معنای رضایت کاربر به پردازش آن اطلاعات یا سوءاستفاده از آن‌ها از سوی شبکه‌ها یا دیگران نیست.

نکته آنجاست که اگر کاربران تنظیمات حریم خصوصی را تغییر ندهند، تدابیر حریم خصوصی بی معنا خواهد بود. علت اصلی عدم تغییر، کمبود زمان، پیچیدگی تنظیمات و بیم از به‌هم‌ریخته شدن پروفایل است. درواقع، ساختار پیچیده تنظیمات حریم خصوصی که درک آن را برای کاربران دشوار ساخته و اهمال کاربران و عدم آگاهی کامل ایشان نسبت به اهمیت موضوع حریم خصوصی در شبکه‌های اجتماعی سبب شده که خودتنظیمی‌ها در این حوزه با شکست مواجه شود.

نتیجه

امروزه شبکه‌های اجتماعی مجازی زندگی انسان‌ها را دردو بعد مثبت و منفی تحت تأثیر قرار داده‌اند. این شبکه‌ها، کاربران زیادی دارند که مشاهده پروفایل خود را برای دیگران میسر ساخته‌اند و از این طریق میزان قابل توجهی از داده‌های شخصی آن‌ها در دسترس عموم قرار گرفته است.

بررسی‌ها نشان می‌دهد که کاربران آگاهی اندکی از تهدیدهای واقعی در فضای مجازی دارند و از میزان افشای اطلاعاتی که سبب نقض حریم خصوصی ایشان می‌شود بی‌خبر هستند و از این‌رو، نگرانی خاصی در مورد شبکه‌های اجتماعی مجازی ندارند و بسیاری از اطلاعات خود را در شبکه‌های اجتماعی مجازی قرار می‌دهند.

شبکه‌های اجتماعی و اشخاص فرصت طلب با طرق مختلف می‌توانند اطلاعات شخصی کاربران و حتی دوستان و خویشان آن‌ها را جمع‌آوری کرده و مورد سوء استفاده قرار دهند.

کلید پیشگیری از نقض حریم خصوصی در شبکه‌های اجتماعی مجازی، نظارت هرچه بیشتر بر آن‌ها و آگاهی بخشی به کاربران این شبکه‌ها است تا شبکه‌های مذکور را فضای امنی برای ذخیره و تبادل اطلاعات خصوصی خود ندانند است. حتی از

131. http://www.facebook.com/full_data_use_policy.

شبکه‌ها می‌توان به عنوان ابزاری هوشمند برای پیشگیری از جرایم و محدود کردن فعالیت‌های مجرمانه و به عنوان ابزار تحقیق و پیگیری در کشف جرایم استفاده نمود. در این راستا، مقامات اجرایی و قضایی بایستی همکاری تنگاتنگی با مالکین شبکه‌ها داشته باشند، کما اینکه فیس بوک مدعی است آمادگی کامل برای همکاری با مقامات قضایی در پرونده‌های آزار و اذیت را دارد و اخیراً سیاست‌های حریم خصوصی خود را اصلاح کرده و تنظیمات ساده‌تری را در نظر گرفته است. با توجه به پیشرفت فناوری به نظر می‌رسد این امکان وجود دارد که همزمان با گسترش خدمات، این شبکه‌ها سعی بر انطباق هرچه بیشتر سیاست‌های خود با قوانین حمایت از داده و افزایش نظارت برسیاست حریم خصوصی خود داشته باشند.

علاوه براین، تصویب اسناد بین‌المللی خاصی در حمایت از حریم خصوصی افراد در شبکه‌های اجتماعی مجازی و مقابله با سایر تهدیدهای ناشی از این شبکه‌ها ضروری است تا همکاری‌های بین‌المللی برای مقابله با این تهدیدها افزایش یابد.

فهرست منابع

فارسی

انصاری، باقر. آزادی اطلاعات. تهران: دادگستر، ۱۳۸۷.

انصاری، باقر. حقوق ارتباط جمعی. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، مرکز تحقیق و توسعه علوم انسانی، ۱۳۸۷.

انصاری، باقر. حقوق حریم خصوصی. تهران: سازمان مطالعه و تدوین کتب علوم انسانی دانشگاه‌ها (سمت)، مرکز تحقیق و توسعه علوم انسانی، ۱۳۸٦.

بای، حسینعلی. بررسی فقهی و حقوقی جرایم رایانه ای. قم: پژوهشگاه علوم و فرهنگ اسلامی، ۱۳۸۸.

سینکلر، ایان. فرهنگ اصطلاحات کامپیوتر و *IT* . ترجمه ابوالفضل طاهریان‌ریزی، تهران: انتشارات طاهریان، ۱۳۸٤.

انگلیسی

Aldinge, Sherry,*Social Networking Sites: How they are used to Perpetrate Criminal Activity and how Law Enforcement uses them as an Investigative Tool,* Florida Department of Law Enforcement Computer Crime Center, June 2008.

Barrigar, Jennifer, *Social Network Site Privacy (A Comparative analysis of 6 sites)*, The office of the privacy commissioner of Canada, februry 2009.

Boyd, d. m., & Ellison, N. B, *Social network sites: Definition, history, and scholarship*, Journal of Computer-Mediated Communication, 13(1), article 11, 2007, Available at: http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

Landis, Cliff, *Friending our Users: Social Networking and Reference Services*, Georgia State University, From the SelectedWorks of Cliff Landis, September 2008.Available at: http://works.bepress.com/clifflandis/3.

Milivojevic, Sanja,*Social Networking Sites and Crime: IsFacebook more than just aPlace toProcrastinate?*, ANZCCC: The Australian and New Zealand Critical Criminology Conference 2010, Available at: http://www.doc-txt.com/Facebook-Social-Networking-

Sites.pdf.
Solis, Brian, *Is Social Media Marketing Recession Proof? The Future Of Media And Communications Starts Here,*Avril 2009, Available at: http://www.briansolis.com/2009/04/is-social-media-marketing-recession.html.
Tsaoussi, Aspasia, *Facebook,*
*Privacy and the Challenges of Protecting Minors on Social Networking Sites,*April 2011, Available at SSRN: http://ssrn.com/abstract=1878035 or http://dx.doi.org/10.2139/ssrn.1878035.
Tuunainen, Virpi Kristiina & Pitkänen, Olli & Hovi, Marjaana, *Users' Awareness of Privacy on Online Social Networking sites – Case Facebook*, 22nd Bled eConference eEnablement: Facilitating an Open, Effective and Representative eSociety, Bled, Slovenia, June 14 – 17, 2009.

فرانسوی

Balagué, Christine & David Fayon, *À quoi sert un réseau social?*2010, Availableathttp://www.pearson.fr/resources/titles/2744100844510/extras/6419_chap02.pdf.
Collée, Laurent, *Sécurité et vie privée sur les réseaux sociaux,* Mémoire de Master en Gestion de la sécurité des systèmes d'information, Faculté de Droit, d'Economie et de Finance de l`université du Luxembourg, 2009.
Coumet, Catherine, *DONNÉES PERSONNELLES & RÉSEAUX SOCIAUX*, Mémoire de master de droit des médias et des télécommunications, Aix-en-provence, 2008-2009.

اسناد

Convension for the Protection of Individuals with Regard to Automatic Processing of Personlal Data, Last visited 23 June 2012, Available at : http://conventions.coe.int/treaty/en/treaties/html/108.htm
Directive 2006/24/EC 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,Last visited 23 June 2012, Available at : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:en:HTML
Directive Concerning Processing of Data and the Protection of Privacy in the Electronic Communication Sector, Last visited 23 June 2012, Available at : http://europa.eu/legislation_summaries/information_society/legislative_framework/l24120_en.htm.
Directive on Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data, Last visited 23 June 2012, Available at : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.
Draft Resolution on Privacy Protection in Social Networking services,Last visited 23 June 2012, Available at : http://www.privacyconference2011.org/htmls/adoptedResolutions/2008_Strasbourg/2008_E5.pdf.
Report and Guidance on Privacy in Social Network Services, "Rome Memorandum" - *43rd meeting, 3-4 March 2008, Rome (Italy)*, Last visited 23 June 2012, Available at : www.datenschutz berlin.de/.../461/WP_social_network_services.pdf
The Granada Charter of Privacy in a Digital World, Granada (Spain), Last visited 23 June 2012, Available at :www.datenschutz-berlin.de/.../696/Granada_Charter_675_40_11.pdf.
Avis 5/2009 sur les réseaux sociaux en ligne, groupe de travail «Article 29» sur la protection des données, Last visited 23 June 2012, Available at : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_fr.pdf.
Charter of Fundamental Rights of the European Union of 7 December 2000, Last visited 23 June 2012, Available at : http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

وب‌سایت‌ها

www.alef.ir
www.briansolis.com
www.cyberbullying.us
www.isna.ir
www.socialmedia.ir
www.tabnak.ir
www.webcache.googleusercontent.com
www.weblognews.ir

Privacy Protection on Social Networking Sites

Bagher ANSARI (Ph.D.)
Assistant Professor of Media Law, Shahid Beheshti University
Shima ATTAR
Student of Master's Degree in Communication Law, Allameh Tabataba'i University

Today social networking sites such as Face book, MySpace, and Twitter have found global fame and have become important part of a modern life. Millions of people throughout the world have joined these networks and share a great part of their information over these networks every day.

The information that users share on these networks could be misused by the providers of networks or third parties. For example, their private information could be disclosed in online environment or provided to companies for advertisement purposes, or used in other ways. Hence, these networks have become an easy platform of accessing the persons' data and the personal data of users and some people associated with them in these networks are threatened. To control these threats, attempts have been initiated in international and national levels but these attempts have not yet achieved favorable and reliable results. In our country, although threats from these networks have jeopardized security of some users, unfortunately the concerns over violating privacy by these networks or associated people are not yet a serious concern.

Hence, the present paper tires to explain the concept of social networking sites and the way they work (chapter 1), and then study the potential threats that may arise against privacy of people through membership in these networks, and the strategies for protection of people against these threats (chapter 2).

Keywords: social networking sites, privacy, personal data, cyber bullying.

ISSN 1682-9220

Journal of LEGAL RESEARCH

VOL. XII, No. 1 2013-1

S. D. I. L.
The S.D. Institute of Law
Research & Study