Charbel Kareh
PhD – Attorney At Law

www.charbelkareh.com

بيانات مستعملي شبكات التواصل الإجتماعي

ومساهمتها في كشف الجريمة

ان طبيعة شبكات التواصل الإجتماعي التفاعلية، تحثّ المستعملين على وضع حياتهم الخاصة بمتناول العموم. وتختلف درجة العمومية بحسب درجة الإنفتاح المراد من قبل المستعمل نفسه، لكن ما يجهله اغلبية المستعملين بأن بياناتهم، حتى المنشورة ضمن الدوائر الخاصة المحصورة، هي بتناول العديد من الأجهزة، وخاضعة احياناً لتجارة البيانات وفقاً لمبدأ السعر الأعلى.

اولاً: امكانية تحديد الهوية الإفتراضية على شبكات التواصل الإجتماعي

ان مسألة تحديد هوية مستعمل معين على شبكة تواصل اجتماعي هي من اكثر المسائل تعقيداً وصعوبة، وباتت تشغل اليوم العالم الحقوقي بإمتياز. ان شبكة التواصل الإجتماعي تحوي، جملة ما تحويه، العديد من الملفات الرقمية كالمصنفات الفكرية المحمية بموجب قوانين الملكية الفكرية، كما تعطي الفرد امكانية نشر المعلومات التي قد تكون ضارة بأحد الأفراد. لذا، تكتسب مسألة تحديد هوية المستعمل الحقيقية اهمية كبرى، وهي ضرورية لجهة تحديد الفاعل لبعض الجرائم التي قد ترتكب على شبكات التواصل الإجتماعي او خارجها.

مصوّر متوافر عبر الشبكة[1]

ان القرارات القضائية التي عالجت هذا الموضوع لم تتطرق بشكل مباشر الى طريقة تحديد الهوية الحقيقية للمستعمل على الشبكة، التي قد تختلف كلياً عن الهوية الإفتراضية المستعملة من قبل المستعمل. لكن بمناسبة

[1]- http://www.google.com.lb/imgres?hl=fr&tbo=d&biw=1440&bih=785&tbm=isch&tbnid=f2Tmv2N7OGLDwM:&imgrefurl=http://www.thevine.com.au/content/%3Fpage%3D651&docid=EghXHuhpApSu6M&imgurl=http://images.thevine.com.au/resources/IMGDETAIL/facebook-costume-455_100310051239.jpg&w=455&h=290&ei=4Am-UKj6IoeytAbguIDgCw&zoom=1&iact=hc&vpx=1126&vpy=155&dur=501&hovh=156&hovw=241&tx=167&ty=60&sig=105861133405470191540&page=2&tbnh=151&tbnw=231&start=33&ndsp=34&ved=1t:429,r:66,s:0,i:280.

دعوى مقامة على احد الأجراء، تطرّق الإجتهاد الفرنسي لمسألة تحديد الهوية على شبكة التواصل، معتبراً انها تشكّل عنصر تيقظ وتنبه هام في كل مرة يعرض ملف على القضاء ويتصل بإستعمال المعلوماتية.

يعتبر الأستاذ بارين ان المحامين والقضاة ينسون غالباً ان اشكالية تحديد مستعمل انترنت او مستعمل معلوماتية هي من الإشكاليات الأصعب التي قد لا تجد حلولاً لها[٢]. ففي العام ١٩٩٣، قام رسام اميركي من نيويورك بنشر رسماً اسطورياً اصبح قولاً مأثوراً بالنسبة للمعلوماتيين مفاده: انه *« على شبكة الإنترنت، لا احد يعرف بأنك كلباً !»* *« On the Internet, nobody knows you're a dog ! »*. ومغزى هذا القول، انه من السهل جداً خلق هوية افتراضية صورية والقيام بأعمال غير مباحة تحت هذا الإسم او الهوية، دون ان يعرف احد الإسم الحقيقي للفاعل. كما اصبح اغتصاب الإسم او انتحال الهوية من الأمور الشائعة والمستعملة بشكل اعتيادي لغايات ومآرب مختلفة ومتنوعة.

على سبيل المثال، يوجد اكثر من خمسين شخصاً مسجلاً تحت اسم انجلينا جولي على شبكة فايسبوك واغلبهم يضع صورتها على الصفحة الشخصية او الهوية الإفتراضية. من يختبئ وراء من، ومن هو الشخص الذي يتخفى وراء هوية افتراضية على فايسبوك؟ ان الإجابة على هذه الإشكالية هي من الأمور الهامة جداً في مادة المعلوماتية حيث حقل الممكن، اقله على المستوى التقني.

في الحقيقة، ان مسألة تحديد الهوية الحقيقية لمستعمل شبكة تواصل اجتماعي تتطلب على السواء تدخلاً تقنياً وتدخلاً استخباراتياً اكثر منه قانونياً. بالنسبة للتدخل التقني، لا بد من تحديد عنوان بروتوكول الإنترنت لحاسوب المستعمل (IP Address)، وبالتالي معرفة تحديد مكانه الجغرافي عبر مقدّم خدمة الإنترنت المحلّي، وهي

[2]- PARRAIN Francois, Réseaux sociaux, preuve informatique et droit du travail, Disponible à partir du site: http://angledroit.com/Droit-Social/reseaux-sociaux-preuve-informatique-et-droit-du-travail.

مسألة تقنية بحتة ومعقّدة جداً بالنسبة للحقوقيين، ولا تعطي نتيجة مضمونة مئة بالمئة، اذ يمكن ان يكون من استعمل الحاسوب شخصاً غير صاحبه.

اما على مستوى التدخل الإستخباراتي، فلا بدّ من دراسة ملف المستعمل المشتبه به الشخصي وهويته الإفتراضية، والتأكد من ما اذا كان المستعمل قد ارتكب اية هفوة معينة سواء في ملفاته الرقمية كالصور التي ينشرها او في رسائله الإلكترونية او في فيديواته او في لحظه لإمكانية الإتصال به سواء عبر الشبكة او خارجها. ليصار بعدها الى تحليل هذه المعلومات وربطها ببعضها وبيانات الأصدقاء، في محاولة للتوصل الى تحديد العناصر التي تمكّن من تحديد هوية المستعمل.

وفي حال عجز كلا التدخلان عن تحديد الهوية الفعلية للهوية الرقمية الإفتراضية، فلا محال من الإتصال بإدارة موقع شبكة التواصل الإجتماعي المعني وطلب منها المساعدة والتعاون، ويفضّل هنا ان يقوم بالإتصال جهة امنية رسمية مكلّفة بالتحقيق بناءاً على شكوى وفقاً للأصول، وهي برأينا اكثر الحلول واقعية.

ثانياً: مصير البيانات على شبكات التواصل الإجتماعي

هل تساءل احد المستعملين يوماً عن مصير بياناتهم على شبكات التواصل؟ هل هي محفوظة في اياد امينة ام يتم تداولها والإتجار بها احياناً؟ ان الصلات المشبوهة التي تربط شبكة فايسبوك مثلاً بالإدارة الأميركية تطرح علامات استفهام عدة، خاصة لجهة الكم الهائل من البيانات الشخصية التي تحويها هذه الشبكة. في الواقع ان كافة المعلومات الموجودة على فايسبوك يتم ادارتها ومعالجتها مباشرة من قبل الإدارات الحكومية الأميركية التالية:

– وكالة الإستخبارات المركزية الأميركية (CIA): بهدف تعدين البيانات (Data mining)،

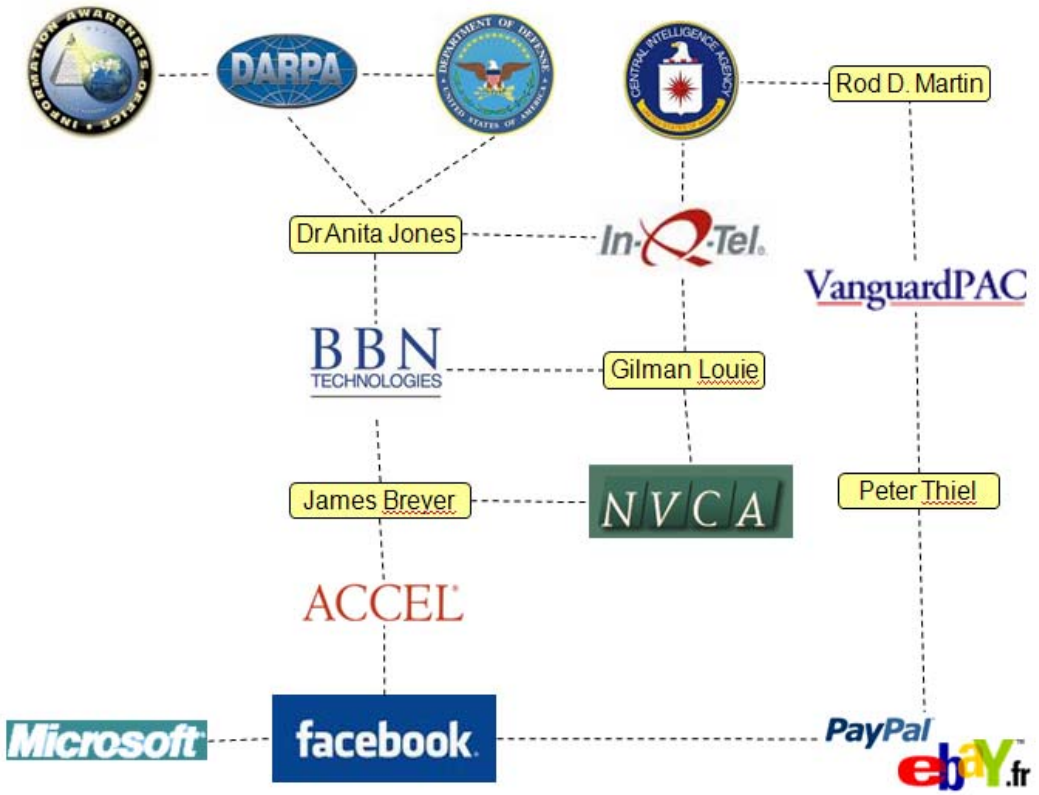
– وزراة الدفاع الأميركية (DOD): بهدف الدفاع والتدرع،

– مكتب الوعي المعلوماتي (IAO): بهدف جمع وتخزين المعلومات التي تخص المواطنين،

– مكتب الأبحاث المتقدمة للدفاع (DARPA): بهدف التحكم بالبشر عن بعد[٣].

ويظهر المصور التالي مدى انغماس شبكة فايسبوك في مشاركتها بيانات الناس الشخصية مع الإدارات الأميركية وغيرها من المؤسسات الخاصة والصلات المختلفة التي تقيمها:

[3]- COLLEE Laurent, Sécurité et vie privée sur les réseaux sociaux, Mémoire Pour l'obtention du diplôme de Master en Gestion de la sécurité des systèmes d'information, Responsable académique : M. Cyril Pierre Beausse Avocat au barreau de Luxembourg Cabinet d'avocats Allen & Overy, Responsable local : M. Jonathan Steele Délégué à la protection des données au Parlement Européen CISSP, Université de Luxemburg, Faculté de Droit, d'Economie et de Finance Master en gestion de la sécurité des systèmes , d'information, Année académique 2009, Disponible sur le site: http://www.cases.public.lu/fr/publications/recherche/Collee/MEMOIRE_SOCIAL_NETWORK_COLLEE_L.pdf, P. 27.



الصلات الغريبة الموجودة بين شبكة فايسبوك والإدارات المعلوماتية الأميركية[4]

في الواقع، ان هوّيات المستعملين تتداخل مع معلومات اخرى متأتية من مواقع اخرى كواقع امازون، ايباي، بايبال، سويفت (Amazon, ebay, Paypal, Swift…) لتضاف على المعلومات الموجودة في قاعدة بيانات الإدارة الأميركية. فيمكن التصوّر، انه في كل مجموعة معلومات، بطاقة كاملة للفرد، لحياته، لمشترياته، لعاداته، لتفضيلاته، لأماكن تمضيته عطلته، لسفراته، لإتصالاته، الخ...

ان شبكة فايسبوك تعلم عن كل فرد اكثر من ما يعرف هذا الفرد عن نفسه. لذلك، يطالب البعض اليوم بأن يصار في كل مرة يريد فيها المستعمل ولوج موقع شبكة فايسبوك الإلكتروني، ان يصار الى سؤاله قبل استعمال الموقع: « كل ما تضيفه على هذا الموقع، يصبح يوماً من الأيام منشوراً للجميع وللآبد، فهل توافق؟[5] ».

[4] - COLLEE Laurent, Op. Cit., P. 27.

ثالثاً: مساهمة بيانات شبكات التواصل الإجتماعي في كشف الجريمة واحقية الحصول عليها

ان اللجوء الى مواقع شبكات التواصل الإجتماعي من قبل الشرطة وسلطات التحقيق اصبح امراً مألوفاً ورائجاً في العديد من البلدان بغية ايجاد العديد من الخيوط التي تساعد في جلاء الحقيقة. ان استعمال شبكات التواصل من قبل سلطات التحقيق والأمن يهدف الى امران: اولاً، جمع المعلومات ومعالجتها بشكل سرّي او مخابراتي بغية مكافحة الجريمة قبل وقوعها او الحدّ منها، وثانياً، ايجاد الدليل على مشتبه به من اجل ادانته.

بالنسبة لجمع المعلومات، إن طبيعة شبكات التواصل الإجتماعي ترتكز على مبدأ التفاعل المعلوماتي، ويكون من المستحيل على المستعمل التواصل دون الدخول في آلية التفاعل هذه، مما يولّد من دون ادنى شك هذا الكمّ الهائل من المعلومات التي تساعد في كافة الإتجاهات. ان رجال الأمن والتحقيق، يجدون من المعلومات المتوافرة على شبكات التواصل، حتى العامة منها، مصدراً مهماً للتحقيق، اذ يمكن ان يشكّل بداية رسم خطوط عريضة لنمط الشخص الإجرامي ولدوافعه الجرمية. ونرد هنا، بعض الأمثلة على استعمالات سلطات التحقيق الأميركية لشبكات التواصل، من اجل استقاء المعلومات:

– تقوم الشرطة بنشر صور وفيديوات عن ساحة الجريمة من اجل الحصول على المعلومات من المستعملين. اذ ان هذه الصور تبقى لوقت اكبر من التلفاز، وتعطي بالمقابل للمستعملين الوقت الكافي للرجوع اليها للتعليق والتعبير،

– يمكن للمستعملين التمعّن في صورة مشتبه به، اذ يصار الى وضعها من قبل الشرطة على الشبكة، بغية المساعدة في تحديد هويته وموقعه. ويستعمل الأنتربول هذه التقنية من اجل ايجاد الفارّين من العدالة.

---

[5] - Ibidem, P. 28.

– تقوم الشرطة بالبحث عن الصور والأدلّة الأخرى للإثبات، التي يكون المشتبه به قد قام بنشرها على صفحته الشخصية على شبكة التواصل،

– تقوم الشرطة بنصب افخاخ للمجرمين على شبكات التواصل، كإنشاء حسابات وصفحات صورية من اجل ضبط مجرمين معتادين،

– في حالات الجرائم المخطط لها مسبقاً، تقوم الشرطة بتحليل محتويات الحاسوب، وعلى وجه خاص اتصالاته مع شبكات التواصل الإجتماعي بهدف ايجاد الأشخاص الذين تم التواصل معهم.

– تقوم وكالة الأمن الوطني الأميركي « NSA » بتصفية صفحات شبكات التواصل من اجل البحث عن متطرفين...

مصوّر متوافر عبر الشبكة[٦]

6-
http://www.google.com.lb/imgres?start=137&hl=fr&tbo=d&biw=1440&bih=785&tbm=isch&tbnid=c7V44TeVtNWJFM:&imgrefurl=http://www.cybercrimesunit.com/should-schools-use-facebook-to-spy-on-students/&docid=ZAlJvG1A1F6VqM&imgurl=http://www.cybercrimesunit.com/wp-content/plugins/rss-poster/cache/670c9_blackboard_facebook-rule.jpg&w=500&h=334&ei=hAq-

تساعد اليوم المعلومات التي تحويها شبكات التواصل على تحديد نمط، سلوك وعادات الفرد، سواء اكان مشتبه به او موقوفاً. فضلاً عن مساعدتها رجال التحقيق في تحديد بيئة المستعمل انطلاقاً من صلاته وعلاقاته الإلكترونية مع الأصدقاء والغير.

اما استعمال شبكات التواصل الإجتماعي من اجل ايجاد دليل قاطع لإدانة مشتبه به، فهو رائج اليوم في العديد من البلدان. ففي اخر مستجدات شبكات التواصل، تم انشاء وحدات لمعالجة جرائم الحاسوب « Computer crime unit » في عدد من البلدان، بهدف مراقبة الشبكات ولا سيما منها شبكة فايسبوك من اجل تحديد هوية العلاقات بين المشتبه بهم[٧]. في بنسيلفانيا، قامت الشرطة بإستعمال شبكة فايسبوك من اجل تحديد هوية الطلاب الذين اقتحموا ملعب اوهايو لكرة القدم حيث تبيّن ان اثنين منهم ملاحقان بجرائم مختلفة[٨]. كما استعملت الشرطة الأميركية الإثباتات الموجودة على كل من شبكة ماي سبايس ويوتيوب، من صور وفيديوات تظهر أفراد عصابات تحمل الأسلحة الغير قانونية، من اجل توقيفهم.

UM6DEZHLsgaOoYBw&zoom=1&iact=hc&vpx=4&vpy=491&dur=1428&hovh=183&hovw=275&tx=57&ty=71&sig=105861133405470191540&page=5&tbnh=141&tbnw=219&ndsp=37&ved=1t:429,r:37,s:100,i:115.

7- BOGUSZ Charlotte, Le regime juridique applicable aux réseaux sociaux, Mémoire présenté et soutenu en Septembre 2009, Sous la Direction de Monsieur le Professeur Georges Chatillon, Droit Administration et Secteurs Publics, Master II Professionnel – Droit De L'internet Public, Disponible à partir du Site : http://www.univ-paris1.fr/fileadmin/diplome_droit_internet/08-09_Bogusz_memoire.pdf, P. 24.

8- STONEBROOK Martha S. & STUBBS Richard A., Social Networking in Law, Enforcement – Legal Issues, available at: http://www.aele.org/los2010_sm-visual.pdf, P. 10.

"Hold on. I just want to put on Facebook that I'm actually in the process of being mugged, then you can have my BlackBerry!"

مصوّر متوافر عبر الشبكة[9]

في احيان كثيرة، ساهمت شبكات التواصل الإجتماعي في ادانة المتهمين. ففي فيرجينيا، اختفت طالبة لها من العمر ١٧ سنة، وقد تمكّن المحققين عبر التدقيق في لائحة اصدقاء الطالبة على موقع ماي سبايس، من تحديد شخص مشكوك به من بين باقي الأصدقاء. مما حمل المحققين على الإعتقاد بأن الطالبة كانت على علاقة مع هذا الرجل المشكوك به الذي يبلغ من العمر ٣٨ سنة. وانطلاقاً من بيانات موقع ماي سبايس وفايسبوك، تمكّن

[9]- http://www.google.com.lb/imgres?start=393&hl=fr&tbo=d&biw=1440&bih=785&tbm=isch&tbnid=wqfhBZHnMCuDbM:&imgrefurl=http://www.cartoonstock.com/directory/a/armed_robbery.asp&docid=hks8f5SjRnVp4M&imgurl=http://www.cartoonstock.com/lowres/jmp100329l.jpg&w=282&h=400&ei=ywu-UJz-F4jmtQaqxIFQ&zoom=1&iact=rc&dur=232&sig=105861133405470191540&page=12&tbnh=149&tbnw=105&ndsp=38&ved=1t:429,r:6,s:400,i:22&tx=92&ty=82.

المحققون من الربط بين المعلومات وتحديد مكان وجود جثة الطالبة التي تم دفنها بالقرب من المؤسسة الزراعية التابعة لعائلة الرجل المشكوك به، وتم ادانة هذا الرجل تبعاً لذلك[١٠].

كما تم سجن شخص يدعى واين فورستر، له من العمر ٣٤ سنة لإقدامه على قتل زوجته طعناً بسبب اعلان قامت بنشره على صفحة فايسبوك. وعند استجوابه، صرّح لرجال التحقيق، انه صعق لدى معرفته بأن زوجته قامت بتغيير وضعها العائلي على صفحتها على شبكة فايسبوك من متزوجة الى عزباء، فور تركه لها[١١].

اما الموضوع الأبرز، فهو مدى التوفيق بين الحياة الخاصة لمستعملي شبكة التواصل وحق سلطات التحقيق في الحصول على المعلومات حتى الخاصة منها. بحسب الأستاذة بوغوز، يمكن لسلطات التحقيق الولوج حتى الى المعلومات الغير منشورة للمستعملين عبر الطلب من ادارة شبكات التواصل الإجتماعي التي تستجيب للطلب. وتستند الأستاذة بوغوز بالنسبة لإجازة هذه الإستباحة للحياة الخاصة، على قرار وزاري فرنسي يجيز للمحققين الوصول الى هذه المعلومات بهدف كشف الجريمة[١٢].

اننا نعتبر ان حق سلطات التحقيق في الحصول على بيانات مستعملي شبكات التواصل هو ضروري وجوهري، وهي لا تختلف عن بيانات داتا الإتصالات. وبرأينا، ان هذا الطلب لا يكون عبر وزارة الإتصالات، انما عبر ادارة شبكة التواصل، اذ يأتي اشملاً، اوسعاً ومجدياً اكثر. ان مجرد الحصول على كلمات السر التي تمكّن من ولوج حسابات مستعملي شبكات التواصل، ليس الا مضيعة للوقت. اذ لا بدّ من الحصول على البيانات المجدية، المتصلة **والمصفّاة.**

10 - COLLEE Laurent, Op. Cit., P. 60.
11 - Ibidem.
12- Bulletin Officiel du Ministère de la Justice du 30 avril 2008 : Circulaire de la DACG du 12 mars 2008 relative à la présentation générale des dispositions du décret du 15 novembre 2007 modifiant le Code de Procédure Pénale et relatif à l'utilisation des Nouvelles Technologies, Disponible sur le site : http://www.textes.justice.gouv.fr/art_pix/boj_20080002_0000_0003.pdf, In BOGUSZ Charlotte, Op. Cit., P.23.

والا، يمكن ان يصار الى اعطاء الأجهزة الأمنية كلمات السر لمستعملي شبكات التواصل ضمن ضوابط وقيود بشكل يحمي من جهة خصوصية وحياة الأفراد الخاصة، ومن جهة ثانية الحق في كشف الجريمة. كأن تكون هذه الإجازة واقعة على مشتبه بهم محددين، سيما وان الربط بين الهواتف الذكية وشبكات التواصل الإجتماعي اصبح امراً متكاملاً اليوم. بالرغم من اقرارنا بوجود احتمال لا بأس به، من ان تكون هذه المعلومات غير مفيدة للمحققين، سيما في حالات الهويات الكاذبة والإفتراضية، استعمال حواسيب ذات ارقام عناوين تعود للغير، المستعمل المشتبه به موجود في الخارج، اقدام المستعمل على الغاء حسابه او محو بياناته التي لا مجال لإسترجاعها الا عبر الإتصال بإدارة شبكة التواصل... لذلك، ان افضل الحلول تكمن في التواصل مع ادارة الشبكات، بناءً على ترخيص قضائي مسبق، من اجل الربط بين المعلومات المتصلة والحصول على المعلومة **المجدية والمصفّاة** من مصدرها. وهذا ما تؤكده التجربات الغربية على كل حال...