

Charbel kareh
PhD – Attorney At Law
www.charbelkareh.com

اشكالية تحديد هوية المجرم الإلكتروني ومحل اقامته على شبكات التواصل الإجتماعي

هل يمكن تحديد هوية المجرم الإلكتروني ومحل اقامته على شبكات التواصل الإجتماعي، وما هي الأدوات المستعملة لتأكيد الإدانة، وما مدى فعالية التدابير الجزائية بالنسبة للمواقع الإلكترونية الأجنبية؟ ان شبكة الإنترنت هي قبل كل شيء مكاناً للتعبير البشري، مكاناً عالمياً متجاوزاً للحدود الجغرافية، مكاناً لامركزياً حرّاً من التسلط الكامل لإدارة او لدولة معينين، مكاناً غير متجانساً يُمكن كل فرد من التصرف، التعبير والعمل، مكاناً عاشقاً للحرية...

لكن هذا المفهوم يصطدم بمبدأ عدم التعرض لحقوق الغير، فإذا كان استعمال الحرية على الشبكة واجب مكرّس وضرورة مصانة، فيجب ان يمارس هذا الحق ضمن حدود التعبير عن الرأي؛ طبقاً للقاعدة الذهبية الموجودة في مختلف الأديان السماوية التي تقول : « لا تفعل للآخر ما لا تحب ان يفعله الآخر لك ». « Ne fais pas à autrui ce que tu n'aimerais pas que l'on te fasse ».

اشكالية تحديد هوية المجرم الإلكتروني ومحل اقامته على شبكات التواصل الإجتماعي

(دراسة تتضمن تعليق على القرار رقم ٩٢٧ تاريخ ١١/٠٥/٢٠١١)

الصادر عن القاضي المنفرد الجزائي في كسروان)

بقلم المحامي الدكتور

شربل وجدي القارح

هل يمكن تحديد هوية المجرم الإلكتروني ومحل اقامته على شبكات التواصل الإجتماعي، وما هي

الأدوات المستعملة لتأكيد الإدانة، وما مدى فعالية التدابير الجزائية بالنسبة للمواقع الإلكترونية

الأجنبية؟

ان شبكة الإنترنت هي قبل كل شيء مكاناً للتعبير البشري، مكاناً عالمياً متجاوزاً للحدود الجغرافية، مكاناً لامركزياً حرّاً من التسلّط الكامل لإدارة او لدولة معينين، مكاناً غير متجانساً يُمكن كل فرد من التصرف، التعبير والعمل، مكاناً عاشقاً للحرية...¹

لكن هذا المفهوم يصطدم بمبدأ عدم التعرض لحقوق الغير، فإذا كان استعمال الحرّية على الشبكة واجب مكرّس وضرورة مصانة، فيجب ان يمارس هذا الحق ضمن حدود التعبير عن الرأي؛ طبقاً للقاعدة الذهبية الموجودة في مختلف الأديان السماوية التي تقول : « لا تفعل للآخر ما لا تحب ان يفعله الآخر لك »، « Ne fais pas à autrui ce que tu n'aimerais pas que l'on te fasse ».

ان القرار الصادر عن حضرة القاضي المنفرد الجزائري في كسروان موضوع هذا التعليق، قد دخل في صلب تكوين شبكة الإنترنت ومفاهيمها التقنية، اذ نجد ولأول مرّة قرار جزائي لبناني يغوص فيه القاضي الى مفاهيم جد معلوماتية تقنية من تواصل بنيوي للشبكات بعضها مع بعض، مروراً بالإستعانة بعنوان بروتوكول الإنترنت الذي يشكّل الهوية الإلكترونية لكل آلة متّصلة بالشبكة، توصلاً الى ادخال عناصر أدلة واثبات جديدة لم يسبق ان رأيناها في قرارات جزائية ضمن فقرة سرد الأدلة، الا وهي « اجهزة الكمبيوتر ومحتوياتها - صفحات الإنترنت »، بالرغم من تحفظنا لجهة ضرورة التفريق بين العتاد المعلوماتي « Hardware » والمعلومات المخزّنة عليه « Data » التي تتشكّل الأدلة المراد الركون اليها.

¹ - THERY J-F, FALQUE-PIERROTIN I, Internet et les réseaux numériques, étude adoptée par l'Assemblée générale du Conseil d'Etat le 2 juillet 1998, La Documentation française, 1998, Disponible sur le site : <http://lesrapports.ladocumentationfrancaise.fr/BRP/984001519/0000.htm>.

سنبدأ تحليلنا بالتكلم عن مفهوم عنوان بروتوكول الإنترنت وأهميته في التوصل الى تحديد مقترف الجرم على شبكة الإنترنت في مرحلة اولى (اولاً)، لننتقل بعدها الى دراسة ادوات اثبات الإدانة والأدلة المسندة اليها (ثانياً)، لنصل ختاماً الى تحديد فعالية التدابير الجزائية المقررة بالنسبة لشبكات التواصل (ثالثاً).

اولاً: اهمية عنوان بروتوكول الإنترنت IP Address في تحديد هوية المستعمل

ان مسألة تحديد هوية مستعمل معين على شبكة تواصل اجتماعي هي من اكثر المسائل تعقيداً وصعوبة، وياتت تشغل اليوم العالم الحقوقي بامتياز. فهي ضرورية لجهة تحديد الفاعل لبعض الجرائم التي قد ترتكب على الويب، منها اعمال جرمية ومنها مثلاً اعمال غير مباحة كالتعرض او خرق الملكية الفكرية لمؤلف معين.

ان القرارات القضائية حتى الأجنبية منها، التي عالجت هذا الموضوع لم تتطرق بشكل مباشر الى طريقة تحديد الهوية الحقيقية للمستعمل على الشبكة، التي قد تختلف كلياً عن الهوية الافتراضية المستعملة من قبل المستعمل. لكن بمناسبة دعوى مقامة على احد الأجراء، تطرق الإجتهد الفرنسي لمسألة تحديد الهوية على شبكة التواصل، معتبراً انها تشكل عنصر تفيظ وتنبه هام في كل مرة

يعرض ملف على القضاء ويتصل بإستعمال المعلوماتية سواء اكان المدعى عليه اجيراً ام صاحب عمل.

ويعتبر الأستاذ بارين ان المحامين والقضاة ينسون غالباً ان اشكالية تحديد هوية مستعمل انترنت او مستعمل معلوماتية هي من الإشكاليات الأصعب التي قد لا تجد حلولاً لها². في 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. ولا بل اكثر من ذلك، اذ 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 الافتراضية. من يختبئ وراء من، ومن يتخفى خلف هوية افتراضية على فايسبوك؟ كيف يمكننا التأكد من هوية الشخص الفعلية للفاعل الذي اقدم على افعال غير مباحة على شبكة التواصل؟ عن من صدر فعلياً بريداً الكترونياً او

²-PARRAIN François, 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>.

رسالة الكترونية مطبوعة على مستند مادي؟ هل تم ارساله لشخص محدد ام للعموم؟ وكيف امكن الإثبات ان خلف هذا الحاسوب، يوجد شخصاً فاعلاً لأعمال غير مباحة؟

ان الإجابة على هذه الإشكاليات هي من الأمور الهامة جداً في مادة المعلوماتية، حيث حقل الممكن، اقله على المستوى التقني، هائل جداً. بالنسبة للأستاذ بارين، من المستحيل اعتبار الإثبات الإلكتروني اثباتاً كاملاً، اذ يمكن تحويل حتى المواقع الإلكترونية التابعة للإدارات العامة، ويمكن التقاط بريد الكتروني تابع للدول، حتى انه تم التقاط خطوطاً دبلوماسية بالكامل ونشر اتصالاتها في السابق... فالأدوات التكنولوجية تسمح للشخص الذي يمتلك معرفتها، بالسيطرة على كل ما يريد من معلومات والتصرف بها كما يشاء³.

في الواقع، ان هوية الشخص هي الأساس في تواجد الشخصية القانونية. مع دخولنا العصر الرقمي، اخذت الهوية الإنسانية بعداً جديداً، وهو البعد الرقمي الذي اخذ نجاحاً مهماً مع شبكات التواصل الإجتماعي. ان الهوية الحقيقية في عصر الويب ٢.٠ هي في خطر التحوّل والإستبدال بالهوية الرقمية. وتعتبر الأستاذة كومي انه تم نقل العديد من اعمال الحياة القانونية الى العالم الافتراضي، التي بدت مشابهة، لكنها تحمل العديد من الإختلافات المتعلقة بالطبيعة الرقمية للشبكة. فالهوية الافتراضية الرقمية هي اوسع بكثير من الهوية الحقيقية⁴.

³-PARRAIN François, 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>.

⁴ - COUMET Catherine, Données Personnelles & Réseaux Sociaux, Mémoire Pour L'obtention D'un Master Recherche « Droit Des Médias Et Des Télécommunications », Sous La Direction De M. Le Professeur Jean Frayssinet, Institut De Recherche Et D'études En Droit De L'information Et De La Communication, Faculté

ان ابرز ما يميّز الهوية الرقمية عن الهوية الحقيقية هو ادخالها بعض المعطيات الجديدة، الغير مألوفة في العالم المادي، كبيانات الإتصال وعنوان بروتوكول الإنترنت « IP Address »، وهذا ما دفع الفقه بتسميتها بالهوية الرقمية. ويرى الأستاذ مورون انها تمثيل تقني للشخص ولأعماله في العالم السيبرالي؛ وهي الأقرب الى هوية الشخص الحقيقية التي تترجم اعماله الى بيانات رقمية^٥.

ان الهوية الحقيقية تركز على معايير جوهرية بسيطة مثل الإسم، العائلة، رقم السجل، العنوان، اسم الوالدة، اما الهوية الرقمية فتستند على معايير اكثر تعقيداً. لكن ما هي هذه المعايير التي تمكن من تحديد الشخص وراء الهوية الرقمية على شبكة التواصل الإجتماعي؟

ان الإجتهاد الفرنسي ليس مطابقاً للساعة حول هذه المعايير المحددة للهوية الرقمية. ففي قراران لكل من محكمة استئناف باريس^٦ ومحكمة الدرجة الأولى في باريس^٧، تم اعتبار انه يجب تقديم عنوان بروتوكول الإنترنت، البريد الإلكتروني واسم المستعمل على الشبكة من اجل التعرف على المستعملين

De Droit Et De Science Politique d'Aix-Marseille, Université Paul Cézanne U III, Aix-En-Provence, 2008-2009, Disponible à partir du site: <http://junon.univ-cezanne.fr/u3iredic/wp-content/rapports-memoires/internet/memoire-coumet.pdf>, P. 59.

⁵ - MOURON P., Internet et identité virtuelle des personnes, Revue de la recherche juridique – Droit prospectif, n°124, 2008.

⁶ - Cour d'Appel de Paris, Ordonnance, 7 janvier 2009, Raphaël Mezrahi et autres/Youtube Inc. Dans cette affaire, des vidéos contrefaites de sketches de l'humoriste ont été diffusées sur le site communautaire. Le juge a donc ordonné à Youtube de transmettre au demandeur les données identifiant les éditeurs.

⁷ - Tribunal de Grande Instance de Paris, Ordonnance de référé, 7 janvier 2009, Jean-Yves Lafesse et autres/Youtube Inc. Les faits sont identiques à ceux jugés le même jour par la Cour d'appel de Paris.

المقلّدين. فيصار إذاً الى استكمال بيانات الهوية الحقيقية بعنوان الإنترنت بروتوكول IP Address «
» اذا كان عنوان الإنترنت بروتوكول غير قابلاً للتزوير، فهو يساهم في تحديد هوية المشترك في
خدمة الإنترنت وليس بتحديد مستعمل الشبكة. وفي قرار لمحكمة بداية باريس، اعتبر مورّد خدمة
الإنترنت ملزم بالإحتفاظ بإسم، عائلة، عنوان وارقام الهاتف للناشرين. في الوقائع المادية، اعتبرت
المعلومات التي يحوز عليها المورّد، من عنوان إنترنت بروتوكول، عناوين بريد إلكتروني، وأسماء
مستعملة للولوج من قبل الناشر، غير كافية⁸.

ان عدم إستقرار الإجتهد حيال موضوع تحديد الهوية الرقمية، جعل من الصعب اعطاء تعريف
واضح لهوية الشخص الرقمية. فإذا كانت البيانات الشخصية، من اسم وعائلة، هي من عناصر
الهوية الرقمية الأساسية، يبقى ممكناً ادخال عليها عناصر جديدة بكل سهولة. فإذا سلمنا جدلاً بأن
جزءاً من الإجتهد يعتبر ان ارقام الهاتف وعنوان السكن هي من عناصر الهوية الرقمية، يبقى انها
من الشروط المنازع بها بسهولة. اذ يمكن ان يقوم المستعمل بكل بساطة بإدخال بيانات غير
صحيحة لدى طلبه الإشتراك بخدمة اتصال بشبكة الإنترنت.

في المقابل، يكون من الصعب جداً، ان لم نقل من المستحيل، ان يقوم مشترك بخدمة انترنت بتزوير
او بإستبدال عنوان بروتوكول انترنت « Address IP »؛ لكن الإشكالية تكمن في ان عنوان

⁸ -Tribunal de Grande Instance de Paris, 14 novembre 2008, Jean-Yves L. et autres / Youtube et autres. Dans cette affaire, des vidéos contrefaites de sketches de Jean-Yves Lafesse ont été diffusées sur Youtube. L'humoriste a donc saisi le juge afin d'obtenir les données identifiant les éditeurs contrefacteurs.

بروتوكول الإنترنت هذا، انما يحدد المشترك في خدمة الإنترنت وليس المستعمل، الذي قام بتزوير الهوية او بإرتكاب الأعمال الجرمية على شبكة التواصل الإجتماعي.

ان تحديد المشترك بخدمة الإنترنت يكون عنصراً مهماً في تحديد نقطة الإنطلاق في التحقيق القضائي، ويكون على المشترك في خدمة الإنترنت الرجوع على المستعمل الذي قام بالعمل غير المباح، وادخاله في الدعوى. لكن، في بعض الأحيان، يكون هذا الأمر ايضاً مستحيلاً، لا سيما في الحالات التي يقوم فيها الأفراد بولوج الشبكة عبر حواسيب عامة، او انطلاقاً من شبكات عامة او مكتبات موضوعة بتصرف الجمهور. فيكون من الصعب جداً تحديد هوية المستعملين، كما ان عنوان بروتوكول الإنترنت، خاصة الشبكة العامة، لا يساعد في هذه الحالة في الوصول الى المستعمل المسؤول عن الفعل الضار.

في النتيجة، ان عنوان بروتوكول الإنترنت هو من الأمور الجوهرية، التي تؤدي الى امكانية تحديد المستعمل، بخلاف كافة البيانات الشخصية الأخرى التي يمكن تزويرها. على شبكات التواصل الإجتماعي، يكون دور ادارة الشبكة جوهرياً بغية التعاون مع الضحية تمهيداً: اولاً لحجب الفعل الضار وثانياً لتحديد الفاعل عبر عناصر تقنية عدة، منها التحديد الجغرافي ومنها هفوات اخرى قد يقوم بها المستعمل. فشبكات التواصل الإجتماعي ليست، الا وسيلة للإعلان عن حياة المستعمل الخاصة، عبر حثه على نشر ما يملك من صور وملفات اضافة الى حالته، عواطفه، مشاعره، رغباته، نشاطاته ونمط عيشه، وكل ذلك يساعد حتماً المحققين في الربط بين المعطيات المختلفة بغية

تحديد الشخص المطلوب. وعلى كل حال، ان التعاون مع ادارة شبكات التواصل يساعد كثيراً في كشف حقائق اساسية قد تحدد هوية الشخص، لكن يبقى خاضعاً لإستتساب شبكة التواصل.

ثانياً: ادوات إثبات الإدانة

بالعودة الى القرار موضوع التعليق، فنجد ان النيابة العامة وحسناً فعلت، ان كلفت مكتب مكافحة الجرائم المعلوماتية وحماية الملكية الفكرية التحقيق، حيث قام هذا المكتب بتوجيه كتاب الى شركة فايسبوك من اجل الإستحصال على IP Log اي عنوان بروتوكول الإنترنت او بمعنى آخر رقم الحاسوب الذي تم من خلاله الإتصال بشبكة الإنترنت فشبكة فايسبوك. ومن خلاله تمكن المكتب من تحديد الشركة موردة خدمة الإتصال بالشبكة في لبنان وهي شركة «Fast Net»، التي بدورها زودت المكتب بهوية الفاعل وعنوان سكنه الخ من بيانات تفصيلية، وتم بالتالي توقيف المجرم استناداً الى ال IP Address او عنوان بروتوكول الإنترنت.

عبر قراءة مضامين القرار موضوع تعليقنا، يتبين ان مسألة تحديد الهوية الحقيقية لمستعمل شبكة تواصل اجتماعي تتطلب على السواء تدخلاً تقنياً (IP Address) وتدخلاً استخباراتياً. بالنسبة للتدخل التقني، لا بد من التمكن من تحديد عنوان بروتوكول الإنترنت للمستعمل (IP Address)، وبالتالي معرفة مكانه الجغرافي عبر مقدّم خدمة الإنترنت المحلي، وهي مسألة تقنية بحتة ومعقدة

جداً بالنسبة للحقوقيين. علماً ان تحديد عنوان بروتوكول الإنترنت للمستخدم، لا يؤدي الى تحديد هوية الفاعل على شبكة الإنترنت بنسبة ١٠٠%.

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

وفي حال عجز كلا التدخلان عن تحديد الهوية الفعلية للهوية الرقمية، فلا محال من الإتصال بإدارة موقع شبكة التواصل الإجتماعي المعني وطلب منها المساعدة والتعاون، ويفضّل هنا ان يقوم بالإتصال جهة امنية رسمية مكلفة بالتحقيق بناءً على شكوى وفقاً للأصول. وفي اغلب الأحيان، تتعاون شبكة التواصل مع الجهات الأمنية/القضائية، أولاً: بغية وقف الضرر الحاصل وحجب او ازالة المعلومات، ولا يحصل ذلك الا اذا تأكد الموقع من صحة المعلومات وتأكد من موضوعية الأضرار الواقعة... ثانياً، عبر التزويد بالمعلومات التقنية المعلوماتية، التي تساعد على تحديد هوية الفاعل وبالتالي الهوية الرقمية، خاصة وان اغلب شبكات التواصل تستعمل انظمة معلوماتية قادرة على تحديد الموقع الجغرافي لأي مستعمل.

لكن اهم ما ورد في هذا القرار موضوع تعليقنا، هو اضافته الى باب الأدلة التقليدية من ادعاء النيابة العامة والقرار الظني، التحقيقات الأولية، اقوال المتنازعين والشهود، **جهاز الكمبيوتر العائد للمدعى عليه، الصور وصفحات الإنترنت المبرزة...**

إذاً، استند القرار المذكور بشكل كبير على جهاز الكمبيوتر ومحتوياته من معلومات رقمية وملفات كما والى معلومات شبكة الإنترنت الخاصة بالظنين من اجل اثبات الإدانة. فأمام القضاء الجزائي تطبق قاعدة حرية الإثبات يقابلها قناعة القاضي الشخصية، وما ذهب اليه القرار المذكور انما في مكانها الصحيح لجهة استحالة ادانة المدعى عليه الا باللجوء الى محتويات حاسوبه الشخصي من ملفات ذات صلة كبيرة وكلها تشكّل المواد الجرمية الممهدة والمنفذة للجريمة. سواء اكان لجهة الملفات والصور الجنسية المنشورة او المراد نشرها والمنسوبة للمدعية، ام لجهة الحسابات المنشأة على شبكات التواصل بإسم ورقم هاتف المدعية بهدف الإضرار بها معنوياً والنيل من مكانتها.

لكننا وعلى مستوى تقني بحث، اننا نرى انه كان من المفضل تسمية الأشياء بأسمائها، كالتفريق مثلاً بين العتاد « Hardware » والبيانات الرقمية على انواعها الذي يحويها هذا الكمبيوتر، ولو استند القرار على المعلومات الموجودة على جهاز الكومبيوتر في فقرة الأدلة لكان حسناً فعل تماماً كما تمت الإشارة الى صور وصفحات الإنترنت.

في الواقع، اننا نعتبر ان مجرد النفاذ من عنوان بروتوكول الإنترنت الى هوية المستعمل الحقيقية، يكون كافياً لإقامة الدليل على ادانة المستعمل، الذي قام بنشر المحتويات الضارة على صفحات شبكة الإنترنت وشبكات التواصل الإجتماعي. وما قام به مكتب مكافحة الجرائم الإلكترونية هو من اجل التوقيف والضبط الحسي للأدلة من جهاز كومبيوتر والاداتا الموجودة عليه. اما الأهم، فهو المعلومات غير المنشورة للعموم والتي جاءت لتجزم ادانة المدعى عليه، كالرسائل الموجودة في بريده الإلكتروني وغيرها من الملفات المرقمة بإسم المدعية والتي كان ينوي استعمالها في المستقبل ونشرها على الشبكة.

في النتيجة، لقد احسن القرار المذكور في اسناد عناصر الأدلة، اذ نرى بوضوح في باب القانون استناده الى أدلة رقمية بشكل كامل، اذ لا يوجد دليل واحد يخرج عن الطابع الإلكتروني للمواد، بدءاً من (١) عنوان بروتوكول الإنترنت (IP Address، ٢) الصور الرقمية المحفوظة على الحاسوب، (٣) الرسائل الإلكترونية المتعلقة بحساب التشهير، (٤) الحساب الإلكتروني المفتوح بإسم المدعى عليها، (٥) امتناع المدعى عليه من تسليم الكومبيوتر، واخيراً الدافع الأهم للجريمة المتمثل بطرد المدعية للمدعى عليه من العمل قبيل مباشرته عمله الجرمي الإلكتروني^٩.

ونشير هنا الى ما جاء في عدة مقابلات لرئيس مجلس القضاء الأعلى، الرئيس جان فهد، حول ضرورة امتلاك القضاة للمعرفة في المعلوماتية والتكنولوجيا الحديثة من اجل التمكن من الفصل في

^٩- لمزيد من المعلومات حول استعمال شبكات التواصل من اجل اثبات الإدانة، راجع قانون الإنترنت، الدكتور شربل وجدي القارح، الجزء الخامس، قانونية التصرفات على شبكات التواصل الإجتماعي، صادر، المنشورات الحقوقية، ٢٠١٣، ص. ١٧٢ وما يليها.

الدعاوى المتصلة، وهذا ما اثبته القرار موضوع هذا التعليق، اذ لم يكتف بالإستناد الى ادلة جميعها رقمية للخروج بالإدانة، بل رد طلب تعيين الخبير لعدم اللزوم والجدوى كما واعتبر احتمال وجود قرصنة غير معزز بالأدلة، وهو شوط متقدّم من الخبرة والإلمام بالمعلوماتي من قبل القاضي مصدرّ هذا القرار.

**ثالثاً: مفعول القرار الجزائري بالنسبة لكل من شركة فايسبوك Facebook وشركة Tagged
وصلاحية مكتب الجرائم المعلوماتية في تنفيذ مضمونه**

بعد ان فنّد القرار بشكل صحيح الأدلة من اجل اثبات الإدانة، وبعد ان اسند قناعته بشكل رئيسي على الأدلة الإلكترونية توصلاً لمسائلة المدعى عليه، بقي عليه انتقاء النصوص القانونية التي تتناسب وفعل المدعى عليه. في قانون العقوبات اللبناني، لم يكن يوجد أي نص يعاقب على اغتصاب الهوية الرقمية بتاريخ اصدار الحكم، مما دفع بالقاضي البحث عن نصوص ذات صلة كجرح النّم والقذح والتشهير، الحض على الفجور، التعرض للآداب والأخلاق العامة، وهذا ما لجأ اليه القرار موضوع التعليق.

ان هذا الأمر يفرض على المشرّع اللبناني اعطاء القضاء المواد القانونية التي تسهّل عمله، اذ اصبح من الضروري ادخال تعديلات اضافية على قانون العقوبات اللبناني، لجهة لحظ جرائم

اغتصاب الهوية الرقمية بشكل صريح، اذ ان تجريم الدخول الى نظام معلوماتي في المادة ١١٠ من قانون المعاملات الالكترونية وما يليها، بما في البقاء في النظام والتعديل فيه تبقى غير كافية لردع هذا النوع من الجرائم.

وقد نصت المادة ١١٠ من قانون المعاملات الالكترونية والبيانات ذات الطابع الشخصي رقم ٢٠١٨/٨١، انه « يعاقب بالحبس من ثلاثة أشهر إلى سنتين وبالغرامة الجناحية من مليون إلى عشرين مليون ليرة لبنانية أو بإحدى هاتين العقوبتين كل من أقدم، بنية الغش، على الوصول أو الولوج إلى نظام معلوماتي بكامله أو في جزء منه أو على المكوث فيه. تشدد العقوبة إلى الحبس من ستة أشهر إلى ثلاث سنوات والغرامة الجناحية من مليونين إلى أربعين مليون ليرة، إذا نتج عن العمل إلغاء البيانات الرقمية أو البرامج المعلوماتية او نسخها أو تعديلها أو المساس بعمل النظام المعلوماتي ». «

اما المادة ١١٢ من القانون عينه، « فتعاقب بالحبس من ستة أشهر إلى ثلاث سنوات وبالغرامة الجناحية من ثلاثة ملايين إلى مئتي مليون ليرة لبنانية أو بإحدى هاتين العقوبتين، كل من أدخل بيانات رقمية، بنية الغش، في نظام معلوماتي وكل من ألغى أو عدّل، بنية الغش، البيانات الرقمية التي يتضمنها نظام معلوماتي ». «

في التدابير التي اقراها القرار موضوع تعليقنا، فنجد اقراره لتدابير يستحيل تنفيذها من قبل جهات لا تأتمر الا بسلطتها الإستتسابية كشركة فابيسوك وشركة TAGGED ذات المركز الرئيسي في ولاية كاليفورنيا الأميركية. وقد سبق لنا حتى في دراسات نشرت في مجلة العدل ان عرضنا لكيفية ازالة محتوى ضار وللآليات المطبقة (Safety Center Policy)، ومدى اعارة شبكات التواصل الأميركية اهمية للقرارات القضائية اللبنانية. فهي خاضعة للدستور وللقانون الأميركي وللقيم والآداب والأنظمة العامة الأميركية المغايرة تماماً للنظام العام اللبناني، وتتص في شروطها العامة على الإستتسابية في تطبيق الأحكام الصادرة خارج ولاية كاليفورنيا.

في الفقرة الحكمية، قضى القرار موضوع التعليق في الفقرة السابعة : « بإقفال الموقع الإلكتروني المفتوح بإسم المدعية على حسابات Facebook و Tagged، وابلغ شركة Facebook ومن يلزم بذلك عبر الأجهزة المختصة ». بعد ان كان قد كلف في متن القرار مكتب مكافحة الجرائم الإلكترونية ابلاغ من يلزم... تبعاً لذلك، هل يمكن لقرار جزائي لبناني إلزام شركة فابيسوك بإقفال حساب على موقعها الإلكتروني؟

في الحقيقة، ان كل من شركة فابيسوك وشركة Tagged، لا تكثرث لأي قرار قضائي صادر خارج ولاية كاليفورنيا كونه لا يحوز على الصلاحية القضائية « Jurisdiction » لمحاسبتها او لإلزامها بأية تدابير. وهذا ما يقع فيه العديد من القرارات القضائية اللبنانية، اذ سبق ورأينا كيف ان قرار قاضي الأمور المستعجلة في بيروت القاضي بسحب فلم « براءة المسلمين » عن شبكة

YouTube، لم يصل الى نتيجة بسبب رفض الشبكة الإلتزام؛ كما رأينا العديد من القرارات الصادرة عن قضاء العجلة القاضية بإقفال حسابات على شبكات التواصل بقيت حبراً على ورق بسبب عدم التزام شبكات التواصل بها^{١١}.

في النتيجة، ان الحلول المجدية من أجل التوصل الى سحب المحتويات الضارة على شبكات التواصل، تكمن في استعمال الآليات الموضوعية من قبل شبكات التواصل والمبنية على اساس القيم الخاصة بالشبكة، والتي يفترض على المستعملين الراغبين في سحب المحتوى اتباعها. ونرد مثال شبكة فايسبوك، حيث تضع بمتناول مستعملها آلية يتم تفعيلها عبر التبليغ عن كل محتوى رقمي ضار، من صور، ملفات، نصوص، تعليقات، منشورات او فيديوات. ليصار بعدها الى تحديد ماهية المحتوى الضار بالنسبة للمستعمل المُبلِّغ.

من ضمن المواضيع الضارة التي على اساسها يصار الى التبليغ، يوجد التبليغ عن مخالفة الملكية الفكرية، عن التعرض الجنسي، عن المضايقة الشخصية، عن المحتويات الإباحية او الجنس ضد القُصْر، الى ما هنالك من مواضيع غير مباحة وفقاً للمصور التالي^{١٢}:

١٠- راجع تعليق على القرار الصادر عن قاضي الأمور المستعجلة في بيروت في ٢٤/٠٩/٢٠١٢ اساس ٢٠١٢/١٠٠٢ (حجب فيلم « براءة المسلمين »)، العدل، السنة ٤٧، العدد ٣، ٢٠١٣، ص. ١٥٣٣.

١١- راجع قانون الإنترنت، الدكتور شريل وجدي القارح، الجزء السادس، المحتوى الرقمي لشبكات التواصل الإجتماعي، صادر، المنشورات الحقوقية، ٢٠١٣، الصلاحية القضائية والحلول المجدية.

١٢ - For more info, see: <https://www.facebook.com/help/www/181495968648557/>.

Facebook Help Center

- Impostor accounts
- Hacked accounts
- Abuse and harassment
- Pages and groups admin issues
- Privacy rights
- Functionality issues
- Usernames and web addresses
- Intellectual property

فئات التبليغ لدى شبكة فايسبوك

بعد تعبئة النماذج الخاصة بالموضوعة على شبكة فايسبوك، يصار الى درس الطلب من قبل الفريق المتخصص بهذا النوع من التبليغ، واذا رأى ان المحتوى المُبلَّغ عنه فعلاً ضاراً ويمس القيم، التعرض للغير، لمكانتهم، لسمعتهم وللمبادئ الموضوعة من قبل الشبكة، يصار عندها الى سحب المحتوى تلقائياً عن الشبكة، لكنه يبقى حكماً في قاعدة بيانات شبكة التواصل اذ انها تملك كافة المعلومات الموجودة على شبكتها.

How to Report Things

Don't have a Facebook account?

[Learn more](#) about how you can report potential abuse on Facebook.

The best way to report abusive content on Facebook is by using the **Report** link that appears near the content itself. Here are some examples of how you can report content to us:

- [Timelines](#)
- [Ads](#)
- [Events](#)
- [Groups](#)
- [Messages](#)
- [Pages](#)
- [Photos & Videos](#)
- [Posts](#)
- [Posts on Your Timeline](#)
- [Questions](#)
- [Something You Can't See](#)

آلية التبليغ عن محتوى ضار لدى شبكة فايسبوك

وفيما يلي نموذجاً عن متابعة قضية خرق ملكية فكرية على شبكة فايسبوك حيث يبدأ التبليغ عنها عبر الموقع الإلكتروني لشبكة فايسبوك وتتابع عبر البريد الإلكتروني:

From: ip+fdzepdu.aeax7sokeukra@support.facebook.com
[mailto:ip+fdzepdu.aeax7sokeukra@support.facebook.com]
Sent: Tuesday, June 11, 2013 10:13 AM
To: ckareh@e-lawyerassistance.com
Subject: Re: Copyright Notification Complaint: #463096730443133

Hi,

Thank you for bringing this matter to our attention. Please note that the channel you have reached is reserved for reporting violations and/or infringements of intellectual property rights, such as copyright or trademark rights.

Based on the information you have provided, it appears that you may be reporting content due to privacy concerns. If this is indeed your intent, and you wish to request the removal of this content from Facebook on that basis, please visit the following Help Center page:

<https://www.facebook.com/help/428478523862899/>

However, if it is instead your intent to report an alleged infringement or violation of intellectual property rights, we would be happy to follow up but need some additional clarification to process your report. Please provide the following:

- Clarification as to what intellectual property rights you believe are being infringed (such as trademark or copyright).
- A description of the exact content that you believe infringes your rights as well as information reasonably sufficient to permit us to locate it. Either provide a link leading directly to the specific content you are trying to report or, if a link isn't available, a detailed description of where it appears on the site, including names of responsible users, dates/times, and/or quotes or descriptions of the content at issue.
- A description of how you believe this material infringes or violates the specific legal rights named above.

After you have provided us with this information, we'd be happy to look into this matter further.

Thanks for your understanding,

Karim
User Operations
Facebook

أذاً، يبقى من الضروري، قبل اقرار تدابير غير قابلة للتنفيذ في القرارات القضائية، معرفة مدى امكانية التزام الجهات المعنية مباشرة في التنفيذ، كإدارة شبكات التواصل الإجتماعي، كما ان الإيعاز لمكتب مكافحة الجرائم الإلكترونية من اجل التنفيذ، انما نجده مقبولاً في الحالة الحاضرة كونه المرجع الذي بادر في طلب عنوان بروتوكول الإنترنت « IP Log » من شبكة فايسبوك. فيكون من المنطقي احالة الطلب اليه من اجل متابعة التنفيذ.

وتجدر الاشارة الى ادخال قانون المعاملات الالكترونية نصوصاً جديدة تحدد القواعد الاجرائية المتعلقة بضبط الأدلة المعلوماتية وحفظها من قبل الضابطة العدلية، حيث عرفت المادة ١٢١ منه

الآثار المعلوماتية، بكونها من قبيل الأدلة الرقمية أو المعلوماتية، وهي البيانات التي يتركها الأشخاص بصورة إرادية أو لا إرادية على الأنظمة وقواعد البيانات والخدمات المعلوماتية والشبكات المعلوماتية. تتضمن الأدلة المعلوماتية : التجهيزات المعلوماتية والبرامج والبيانات والتطبيقات والآثار المعلوماتية وما يماثلها. تتبع القواعد الواردة في هذا الفصل عند ضبط الأدلة المعلوماتية بناءً لقرار النيابة العامة أو المرجع القضائي المختص. يجب احترام الخصوصية لجهة الآثار المعلوماتية ولاسيما البيانات والصور غير المتعلقة بالدعوى الجزائية. تقوم الضابطة العدلية بإجراءات ضبط الأدلة المعلوماتية وحفظها والمنصوص عنها في هذا الفصل، بناءً لقرار المرجع القضائي المختص. يؤازر الضابطة العدلية في ضبط الأدلة المعلوماتية وحفظها مكتب متخصص.

اما المادة ١٢٢ منه، أعطت للمحكمة تقدير الدليل الرقمي أو المعلوماتي وحجيته في الإثبات، ويشترط أن لا يكون قد تعرض لأي تغيير خلال عملية ضبطه او حفظه او تحليله.

علماً انه يمكن لأي صاحب صفة ومصلحة الإتصال بشبكة فايسبوك واعتماد آلية التبليغ المشار اليها اعلاه من اجل اقفال حسابات او سحب محتويات رقمية ضارة، دون اللجوء الى استصدار قرارات قضائية قد تشكل نفيراً او تحدياً لشبكة التواصل التي تعتبر نفسها الحامية الأولى عن للحريات الرقمية على شبكتها؛ الامر الذي يضعنا امام نوع جديد من التشريعات المتحكمة بفضاء الكتروني محدد وشبكات معينة، يمكن تسميتها « بالتشريعات » ذات الطبيعة الخاصة التي تضع

مستخدمي الشبكة امام سلطة الامر الواقع التي تدعن إستعمال الشبكة عبر الزامية الخضوع لكافة احكامه واعرافه وقواعده المطبقة.

*

**

القرار رقم ٩٢٧

صادر بتاريخ ١١/٥/٢٠١١

الهيئة الحاكمة: الرئيس جوزف ابو سليمان

الحق العام وم. ش / ش . س .

- حساب الكتروني - فتح حساب الكتروني على موقع ال انترنت ونسبته للمدعية من اجل التشهير بها - ورود اتصالات بها عبر الموقع من اجل المواعدة الجنسية - النيل من سمعتها وكرامتها - ادلة تثبت ان المدعي هو وراء الفعل المذكور - ارتباك المدعى عليه للتملص من المسؤولية يشكل قرينة على عدم مصداقيته - ادلة مضبوطة على جهاز كمبيوتر المدعى عليه بالتزامن مع حساب التشهير ومع خلاف المدعى عليه مع المدعية - افعال تشكل الجرح المنصوص عليها في المواد ٥٢٦ و ٥٣٢ و ٥٨٤ عقوبات (تعرض للاخلاق العامة - فجور - قدح باحدى وسائل النشر) - اضرار معنوية جسيمة بسمعة وكرامة المدعية - آلام نفسية - ازعاج

نفسى نظراً لموقعها المهني والاجتماعي - تعويض - اصدار الامر لشركة Face book بإقفال الموقع الالكتروني المفتوح على صفحة Taggad باسم ... - ابلاغ من يلزم بواسطة مكتب مكافحة الجرائم المعلوماتية لدى الشرطة القضائية.

بناءً عليه،

في القانون:

حيث انه من الثابت انه تم فتح حساب الكتروني على موقع ال انترنت وتُسبب للمدعية من اجل التشهير بها، مما نال من سمعتها وكرامتها، نتيجة كثرة الاتصالات التي كانت تردّها من اجل المواعدة الجنسية،

وحيث انه تبين ان المدعى عليه هو وراء الفعل المذكور اعلاه بدليل:

١- اكتشاف اسمه عبر متابعة IP ضمن لائحة الزبائن والذي تم من خلاله فتح الحساب.

٢- اكتشاف ذات الصور الاباحية المرسلّة على حساب التشهير على صفحة Desktop على جهاز الكمبيوتر الخاص به مع عبارة Exported ds Mireille مع ملفات باسم /1 Mireille / و /2 Mireille / و /3 Mireille /.

٣- اكتشاف رسائل تتعلق بحساب التشهير وبلاستفسار عن رقم هاتف المدعية الموضوع على حساب التشهير على Inbox خاصة المدعى عليه الذي لا يمكن الولوج اليه الا عبر البريد الالكتروني خاصة المدعى عليه وكلمة المرور خاصة المدعى عليه.

٤- فتح حساب باسم Mireille C على جهازه يتضمن ذات المعلومات الشخصية المدونة عن المدعية في حساب التشهير.

٥- محاولة امتناعه عن تسليم جهاز الكمبيوتر الخاص به المضبوط عند مفاجأته من عناصر التحري من اجل اخفاء الادلة.

٦- مصادفة حصول حساب التشهير بعد تركه العمل لدى المدعية وبعد وقوع الخلاف بينهما.

وحيث انه، وفي ضوء الادلة المذكورة اعلاه، يقتضي ردّ طلب المدعى عليه تعيين خبير لعدم اللزوم والجدوى، كما انه، وفي ضوء الادلة المتوافرة، لا يمكن اعتبار الفاعل مجهولاً، ولا يمكن غض الطرف عن ضلوع المدعى عليه في الافعال الحاصلة،

وحيث ان قول المدعى عليه ان وجود الصور الاباحية والمحادثات والرسائل على جهازه هو مجرد صدفة هو قول غير مقنع وغير معزز بما يؤيده، هذا فضلاً عن انه امام المحكمة ادلى بأن في الامر قرصنة دون اقامة الدليل على قوله الاخير، مما يفيد ارتباك وتخبط المدعى عليه للتملص من المسؤولية وبشكل قرينة على عدم مصداقيته، وفي مطلق الاحوال، لا يمكن اعتبار كل الادلة المضبوطة على جهاز كمبيوتر المدعى عليه بالتزامن مع حساب التشهير ومع خلافه مع المدعية مجرد مصادفة،

وحيث ان قول المدعى عليه بأنه تعرض للاكراه والضغط امام عناصر التحري مردود بعد ان اقر امام المحكمة بأن اجوبته امام عناصر التحري هي صحيحة (ص /٣٣/ من المحضر)، وفي مطلق

الاحوال، فهو انكر في التحقيق الاولي ما نُسب اليه، فلا يفيد به شيء القول بأنه تعرض للضغط والاكراه، فترد اقواله المخالفة لهذه الناحية،

وحيث ان افعال المدعى عليه كما هي موصوفة اعلاه تشكل بالتالي الجرح المعاقب عليها سنداً للمواد /٥٢٦/ و/٥٣٢/ و/٥٨٤/ عقوبات دون الجرح المنصوص عنها في المواد /٥٣١/ و/٥٣٣/ و/٧٥٩/ عقوبات،

وحيث ان المحكمة ترى، وبالنظر للاضرار المعنوية الجسيمة اللاحقة بسمعة وكرامة المدعية وما سببته لها من آلام نفسية عميقة وازعاج نفسي كبير نظراً إلى موقعها المهني والاجتماعي، الزام المدعى عليه بدفع تعويض للمدعية بمقدار ثلاثون مليون ل.ل.،

وحيث انه يقتضي ايضاً، ومن اجل محو آثار الفعل للمستقبل، اصدار الامر لشركة face book بإقفال الموقع الالكتروني المفتوح على صفحة Taggad باسم:

- Mireille ****:

<http://www.facebook.com/home.php?#/profile.php?id=1114386040&ref=nf>

- Mireille ****:

<http://www.facebook.com/profite.php?Id=1608438037&v=feed,ofviewas891845056>

- Mireille C: <http://www.taggad.com/profile.html?uid=5412849946>

وابلاغ من يلزم بواسطة مكتب مكافحة الجرائم المعلوماتية لدى الشرطة القضائية،

لذلك،

يحكم:

أولاً: بإدانة المدعى عليه ش. ي. س. بمقتضى المادة /٥٢٦/ عقوبات، وحبسه لمدة ستة اشهر
وتغريمه مائتي الف ل.ل.، وعلى ان يحبس يوماً واحداً عن كل عشرة آلاف ليرة من الغرامة عند
عدم الدفع.

ثانياً: بإدانة المدعى عليه ش. ي. س. بمقتضى المادة /٥٣٢/ عقوبات، وحبسه لمدة ستة اشهر
وتغريمه مائتي الف ل.ل.، وعلى ان يحبس يوماً واحداً عن كل عشرة آلاف ليرة من الغرامة عند
عدم الدفع.

ثالثاً: بإدانة المدعى عليه ش. ي. س. بمقتضى المادة /٥٨٤/ عقوبات، وحبسه لمدة ثلاثة اشهر
وتغريمه ثلاثمائة الف ل.ل.، وعلى ان يحبس يوماً واحداً عن كل عشرة آلاف ليرة من الغرامة عند
عدم الدفع.

رابعاً: بإبطال التعقبات الجارية بحق المدعى عليه ش. ي. س. سنداً للمواد /٥٣١/ و/٥٣٣/
و/٧٥٩/ عقوبات لعدم تحقق عناصرها بحقه.

خامساً: بإدغام العقوبات عملاً بالمادة /٢٠٥/ عقوبات بحيث لا تنفذ بحق المدعى عليه ش. ي.
س. سوى عقوبة الحبس لمدة ستة اشهر مع احتساب مدة توقيفه من ٢٠٠٩/٢/١٨ وحتى
٢٠٠٩/٣/٣ وتغريمه مائتي الف ل.ل.، كونها الاشد.

سادساً: بإلزام المدعى عليه ش. ي. س. بأن يدفع للمدعية ميراى سمير شوفانى تعويضاً بمقدار ثلاثون مليون ل.ل.

سابعاً: بإقفال الموقع الالكتروني المفتوح باسم Mireille **** و Mireille **** و Mireille C والمبينة ارقامه في المتن على صفحات face book و taggad و ابلاغ شركة face book ومن يلزم بذلك عبر الاجهزة المختصة.

ثامناً: بتدريك المدعى عليه النفقات القانونية.

