THE JOURNALIST SURVIVAL GUIDE

ANANIMATEDVIDEOGUIDE

Samir Kassir eyes

الدرس ٢
حماية هوية المصدر

إنّ حماية هوية المصدر هو أحد أهمّ القرارات وأكثرها خطورةً التي يمكن لأيّ صحافيّ أن يتّخذها.
ففي العديد من الحالات، يأتمنك المصدر على مسيرته المهنية، وسلامة أسرته، لا بل على حياته نفسها.
لذا، قبل أن تتّخذ قراراً كهذا، يجب أن تتّفق مع مصدرك، بأكبر قدر ممكن من الوضوح، على ما يجوز أو لا يجوز لك فعله في سبيل حمايته.
وفوق كلّ ذلك، إيّاك وإطلاق الوعود التي لن تتمكّن من الإيفاء بها.

قبل إجراء المقابلة، حدّد القواعد التي ستلتزم بها عند نقل المعلومات التي ستحصل عليها من المصدر.
هل يجوز لك ذكر اسم المصدر؟
هل يجوز لك تحديد مكان عمله أو منصبه ضمن المنظّمة التي يعمل فيها؟
هل يجوز لك الاقتباس عنه مباشرةً؟
كصحافيّ، من الضروري أن تكشف أكبر قدر ممكن من المعلومات عن مصدرك، لتثبت مصداقيتكما بنظر جمهورك.
عند التفاوض على هذه الشروط، حاول ألا تطرح العديد من الاقتراحات. أترك المصدر يفكّر بنفسه ويقرّر كم من المعلومات سيكشف عنها بشأن هويّته.
تجنّب القول إنك ستكتم هوية المصدر على وجه التأكيد. فمن الظروف ما قد يرغمك على الكشف عنها.
عوضاً عن ذلك، قل إنك ستفعل كل ما في وسعك لتحافظ على سرية هويّته، ثم حدّد كيف تنوي فعل ذلك.
خلال هذه المناقشات، سجّل دوماً الملاحظات بدقة، واحفظها في مكان آمن. إستخدم دفتر ملاحظات واحد لتسجيل كلّ المعلومات المتعلقة بالمصدر السريّ. لكن إياك وتدوين معلومات الاتصال به على هذا الدفتر. إذا أمكن، إحفظ اسمه في ذاكرتك وأشر إليه ضمن ملاحظاتك برقم أو رمز.
لا تتناقش مع أصدقائك أو أسرتك حول هوية مصدرك أو المعلومات التي حصلت عليها منه.

لعلّ أفضل طريقة للحصول على معلومات غير قابلة للتعقّب هي التحدّث إلى المصدر شخصياً في مكان خصوصي. فمن الممكن تعقّب البريد الإلكتروني والرسائل القصيرة والمكالمات الهاتفية.
إحمل معك إلى الاجتماع كاميرا صغيرة الحجم مجهّزة بإمكانية التسجيل بالفيديو، حتى وإن كنت تنوي إجراء المقابلة كاملةً في وقت لاحق. فمن المحتمل ألا يوافق مصدرك على التحدّث معك إلا مرة واحدة فقط. لا تستخدم كاميرا الهواتف الذكية أو أيّ جهاز متّصل بشبكة الإنترنت.
في العديد من الحالات، قد يتعذّر عليك مقابلة المصدر شخصياً، فتضطر إلى التواصل معه إلكترونياً.
استعداداً لذلك، يجب أن تتعرّف أكثر إلى التقنيات المتوافرة لحجب هويّتك.
إستخدم برامج الإنترنت الآمنة، مثل برنامج «تور»، الذي يمكّنك من استخدام الإنترنت كمجهول للهوية وحجب عنوان الآي.بي الذي يعرّف بحاسوبك.
تقدّم غرف الدردشة وخدمات البريد الإلكتروني الآمنة مستوىً معيّناً من الأمن. ولعلّ إحدى أكثر الطرق رواجاً لتشفير المحادثات الإلكترونية، وهي الطريقة التي يمكن أن تستفيد من الانتشار الواسع الذي يحقّقه موقع «فايسبوك»، هي ميزة الدردشة خارج السجل (Off-The-Record)، من خلال إضافة برنامج «بدجن» (Pidgin) للدردشة على جهاز الكمبيوتر الخاص بك.

[http://pidgin.im/] | [https://developer.pidgin.im/wiki/ThirdPartyPlugins]

كما يمكن لمستخدمي جهاز «ماك» أن يحصلوا على خدمات مشابهة، بفضل برنامج المحادثة «أديوم» (Adium) الذي يتضمّن ميزة الدردشة خارج السجل أيضاً. في هذا الإطار، يمكن زيارة موقع encrypteverything.ca، للاطلاع على دليلٍ مفصّل يشرح، خطوةً بخطوة، كيفية تنزيل هذا البرنامج.
ولا بدّ من الإشارة أيضاً إلى خدمة البريد الإلكتروني المشفّر التي يقدّمها بريد «جيمايل» التابع لغوغل، من خلال متصفّح ملحق بـ«غوغل كروم» يُعرف باسم «الجيمايل الآمن» (SafeGmail).
لكن ليس من نظام مكفول تماماً ضدّ الخطأ. وبالتالي يجب أن تفترض دوماً، خلال عملك، أنّ اتّصالاتك الإلكترونية خاضعة للمراقبة، آخذاً

بعين الاعتبار أنّ شخصاً ما قد يسجّل دخوله إليها ويحفظها بالكامل. ولعلّ أشهر الشبكات المعروفة بمستوى أمنها المتردّي هي شبكات الواي فاي (Wi-fi networks). فيكفي أن يضبط المتجسّسون برامج مثل «البريد الآمن» أو خادم «بروكسي» على جهاز الكمبيوتر الخاص بك، كي تساورهم الشكوك بأمرك.

إذا وافق مصدرك على إجراء مقابلة مصوّرة، يمكن اعتماد عدة تقنيات لإنتاج المقابلة على نحو يحمي هويته. ومن أكثرها شيوعاً تقنية تمويه الوجه في مرحلة تحرير وتقطيع الفيديو بعد انتهاء المقابلة. لكن كن حذراً عند القيام بذلك، لأنّ صور شريط الفيديو الأصلي ستكشف، بكلّ تأكيد، عن حقيقة هذا الشخص وشكل وجهه.
أما التصوير «في الظلّ»، فليست تقنيّةً آمنة تماماً. فبمقدور برامج التعرّف إلى الوجه أن تحدّد هوية الأشخاص بكلّ سهولة، استناداً إلى الجانب الأيسر أو الأيمن من وجوههم، لا بل حتى انطلاقاً من شكل آذانهم. حتى وإن بدا الوجه معتماً تماماً على شاشة الكاميرا، فمن المحتمل جداً أن تكشف المناطق المعتمة عن معلومات تفوق ما كنتَ تتصوّره بكثير.
ومن التقنيات الأخرى أيضاً، استخدام أوشحة أو أقنعة لإخفاء كامل الوجه ما خلا العينين. لكن لا يخفى على أحد أنّ العينين تميّزان كلّ شخص عن غيره، وبالتالي سيسهل التعرّف إلى الشخص الذي تجري معه المقابلة عن طريق النظر إلى حدقة العين ليس إلا.
قد تتمكّن من تصوير المقابلة عبر الاستعانة بلقطات لا تظهر وجه الشخص المعنيّ. لكن تنبّه إلى أنّ اللباس، واليدين، لا بل حتى بعض الحركات، يمكن أن تفضح، بدورها، هوية هذا الشخص.
من الحلول الناجعة، إذا كنت تستعين بمصوّر غيرك، توجيه الكاميرا نحوك مع تصوير رأس الشخص المعنيّ في مقدّمة الصورة. أطلب من الشخص ارتداء وشاح أو قبّعة لإخفاء هويته، ولالتقاط صورة لافتة بصرياً في الوقت عينه. إحرص على عدم وجود أيّ موادّ عاكسة يمكن أن تكشف عن وجهه.

إستخدم دائماً كاميرا ذات وسائط قابلة للإزالة، كي تقوم بحفظ الموادّ المسجّلة عليها عوضاً عن حفظها على ذاكرة الكاميرا المركّبة داخلياً.
جديرٌ بالذكر أنّ معظم الكاميرات الحديثة تقوم على استخدام البطاقات المرقّمة الآمنة (SD cards) التي تعتبر مفيدة جداً في حماية موادّك الإعلامية. لذا، من الأفضل أن تحمل معك بطاقتين مرقّمتين على الأقل خلال المقابلة.
حالما تنتهي من تصوير المقابلة، إنزع البطاقة المرقّمة الآمنة فوراً من الكاميرا وضعها في مكان آمن. استبدل البطاقة بأخرى جديدة؛ وعندما تنتهي من العمل مع المصدر، صوّر بعض اللقطات الجديدة، كمشهد في الشارع أو السوق مثلاً. بهذه الطريقة، إذا أوقفك أحدهم وصادر الكاميرا الخاصة بك، ستتمكّن من إعطائه تفسيراً معقولاً لما كنتَ تفعله، خاصّةً وأنّ المادة الجديدة التي صوّرتها ستكون ممهورة بوقت وتاريخ لا سبيل للتشكيك فيهما. أما إذا كانت البطاقة المرقّمة الآمنة فارغة، فستثير الشكوك في نفس أيّ شخص صادر منك الكاميرا.

من عادة صحافيي الفيديو الذين يتعاملون بشكلٍ روتيني مع المصادر السرية استخدام جهازَي كمبيوتر، أحدهما للاستخدام العام والآخر غير متّصل بالإنترنت على الإطلاق. فإذا كنتَ تملك جهازَي كمبيوتر، إستخدم الجهاز غير المتّصل بالإنترنت لاستيراد مادّتك الإعلامية وتحريرها. أما إذا كنتَ تملك جهازاً واحداً فقط، فتجنّب الاتصال بشبكة الإنترنت عندما تعمل على إعداد المواد الإعلامية.
بعد أن تنتهي من عملية التحرير، يصبح بإمكانك تصدير المشروع المكتمل، ومحو الملفّات المتعلقة بالمصدر، فضلاً عن أيّ ملفّات «بروكسي» كنت قد اضطررت إلى إنشائها خلال عملية التحرير. لا تحتفظ في أرشيفك إلا بالبطاقة المرقّمة الآمنة الأصلية فقط. أما إذا كنتَ بحاجة إلى إرسال تقريرك النهائي أو تحميله عبر الإنترنت، فانسخه على أحد وسائط التخزين النقالة، ثم أدرج هذه الأداة في حاسوب متّصل بشبكة الإنترنت.
تبعاً لظروفك، يمكنك ابتكار أنظمة خاصة بك لحماية هوية المصادر السرية. لكن تذكّر دوماً أن تتحلّى بالحذر عند إطلاق الوعود، وأن تلتزم بها دائماً، واستمرّ بتثقيف نفسك عن أحدث التطوّرات التكنولوجية التي يمكن أن تحمي عملك أو، على العكس، تزيد من خطورته.

إنتاج:
مركز الدفاع عن الحريات الإعلامية والثقافية «سكايز» – مؤسسة سمير قصير

تم إعداد محتوى الفيديو بمساعدة من:
فريق تكنولوجيا المعلومات والاتصالات في المعهد الديمقراطي الوطني للشؤون الدولية

المنتج التنفيذي: **مارون صفير**
تصميم وتحريك: **kook creative studio**

مستشار تقني: **أندرو كود**
ترجمة: **نور الأسعد**
صوت (عربي): **ريما خداج**
الصوت (انجليزي): **أندرو كود**
تسجيل الصوت: **Creative Impact**
موسيقى: **«Mining by Moonlight» by Kevin MacLeod**

تم تنفيذ هذا المشروع بفضل دعم **الصندوق الوطني للديمقراطية.**