

تقنيات التوثيق الآمن
للاحتجاجات والانتهاكات

الصوت الأمن
sv.khro.org





الفهرس

- **المقدمة**
- **الفصل الأول:** أخلاق وأمن الكاميرا في الميدان
- **الفصل الثاني:** طرق الإخفاء والتعديل الآمن للصور
- **الفصل الثالث:** التنظيف الجذري للأثر الرقمي
- **الفصل الرابع:** طرق التخزين الآمن والإخفاء السري للمعلومات
- **الفصل الخامس:** طرق الاتصال الآمن وتشفير الحسابات
- **الخاتمة**



المقدمة

في عقيدة الأمن الحديث، يُعد الفصل بين "الأمن في الشارع" و"الأمن في بيئة الشبكة" خطأً استراتيجياً قاتلاً وغير قابل للاسترداد. لقد جعلت الأجهزة القمعية، بما في ذلك شرطة فتا، وزارة الاستخبارات، واستخبارات الحرس الثوري، عملية التحديد والقمع تتحول من حالة تقليدية إلى دورة ذكية متصلة ومبنية على البيانات (Data-Driven). تتكون هذه الدورة من أضلاع أساسية أربعة: تسجيل الصور في الميدان، استخراج الهوية الفيزيائية من خلال الذكاء الاصطناعي، تتبع الأثر الرقمي في شبكات التواصل الاجتماعي، وأخيراً الاعتقال الاستنزافي للنشطاء. في إقليم الأهواز (محافظة خوزستان)، وبسبب تكرار انقطاع الإنترنت الشامل أثناء الأزمات البيئية مثل أزمة المياه ونقل نهر كارون، واحتجاجات المعيشة والمدنية، تواجه توثيق انتهاكات حقوق الإنسان تحدي الإخفاء المنهجي. الهدف من هذا الدليل هو تسليحك تكنولوجياً بطريقة تحول عدسة كاميرتك إلى درع دفاعي؛ بحيث يتم تسجيل الحقيقة ونقلها، ولكن يظل الراوي والموضوع بعيدين عن رادار مراقبة جهاز القمع.



الفصل الأول

أخلاق وأمن الكاميرا في الميدان

التصوير الميداني في المناطق الحرجة ليس مجرد ضغطة على زر التسجيل، بل هو عملية هندسية يجب أن تقدم أقل قدر ممكن من البيانات الوصفية البصرية والهوية للمراقب القمعي.

1.1. تشريح مخاطر الرؤية الآلية (Computer Vision)

أنظمة الرقابة الحديثة وكاميرات تسجيل المخالفات المرورية الحضرية المثبتة في التقاطعات الرئيسية وأحياء إقليم الأهواز لم تعد تعتمد على نظر المشغل البشري. هذه الأنظمة مزودة بخوارزميات متقدمة للتعرف على الوجه (Face Recognition)، التعرف على لوحات السيارات (ANPR)، وتحليل الخصائص الفردية (Soft Biometrics) مثل الطول، شكل الكتف، وطريقة المشي (Gait Analysis).

- بروتوكول التغطية البيومترية في الميدان: استخدام الأقنعة الطبية وحدها غير مفيد؛ لأن ذكاء الرؤية الاصطناعي الرقابي يمكنه تخمين الهوية من خلال مطابقة عظام الجبهة، المسافة بين العينين، وإعادة بناء باقي الوجه. يجب على النشطاء استخدام تقنية الطبقات البصرية:
  - أ) نظارات شمسية معتمة بالكامل وبدون انعكاس لإخفاء محجر العين ونقطة تركيز الأنماط البيومترية.
  - ب) قبعات بيسبول شمسية ذات حافة طويلة لكسر زاوية رؤية الكاميرات المثبتة في ارتفاع عالٍ وخلق ظل على النصف العلوي من الوجه.
  - ج) أقنعة قماشية داكنة اللون وبدون رسومات؛ يجب أن يغطي القناع حتى أسفل الذقن لكي يتشوه شكل الفك (Jawline) تماماً، والذي يُعد أحد المؤشرات الرئيسية للرؤية الآلية.





1.2. سيناريو تحليل انعكاس الضوء (Reflection Forensics)

تُعد واحدة من أكثر طرق تحديد هوية مرسلي الفيديو تعقيداً وأقلها انتباهاً من قبل القسم التقني لشرطة فتا هي تحليل الانعكاسات غير المرغوب فيها في الصور. عند التصوير سراً من خلف نافذة مبنى، داخل متجر، أو من داخل سيارة، يعمل الزجاج كمرآة شبه شفافة. يتم انعكاس صورة وجهك، أو طراز أو لون ملابسك، أو الديكور الداخلي للغرفة على الزجاج وتسجيلها بالتزامن مع المشهد الخارجي. أدوات معالجة الصور عبر تعزيز التباين (Contrast Enhancement) لهذه الأجزاء توصل الضباط مباشرة إلى غرفة أو سيارة المرسل.

- قبل البدء في التصوير من خلف الزجاج، أوقف تشغيل جميع مصادر الإضاءة خلفك تماماً (مصباح الغرفة، شاشة الكمبيوتر، شاشة LCD، التلفزيون، أو الهاتف الثاني)؛ يجب أن تكون الغرفة في ظلام دامس.
- ضع عدسة كاميرا الهاتف بشكل ملتصق تماماً وعمودي على سطح الزجاج. من الضروري استخدام قماش داكن حول العدسة لسد فتحات دخول الضوء الجانبي.
- تجنب التصوير من الهياكل اللامعة للسيارات المتوقفة أو المرايا الجانبية التي قد تسجل أثرك وصورتك.

1.3. ورشة عمل التمويه الصوتي المتخصص

الأصوات فريدة وهوياتية تماماً مثل بصمات الأصابع. يمكن لخوارزميات التجسس الترددي مطابقة البصمة الصوتية للأفراد (Voiceprint) مع بنك معلومات التسجيلات الصوتية لمشغلي الاتصالات (مثل همراه اول وايرانسل). العلامات الجغرافية الصوتية (Acoustic Landmarks) مثل صوت بوق قطار، صوت الأذان من مسجد معين بتردد محدد، صوت محول كهربائي محلي، اللهجة الفريدة للمرسل، أو نداء اسم صغير في خلفية الفيلم، تفضح النطاق الجغرافي وهيئة الشبكة.

- **بروتوكول تشغيلي:** عند تسجيل الفيديو في الميدان، لا تتحدث تحت أي ظرف من الظروف وتواصل مع المرافقين بإشارات اليد. قبل إرسال أو نشر الملف، باستخدام برامج التحرير مثل SoundView أو الأدوات الداخلية لتطبيقات المراسلة، قم بقطع الصوت الأصلي للبيئة تماماً (Mute)؛ يجب ألا يصل أي تردد صوتي أصلي إلى الناتج النهائي.



الفصل الثاني

طرق الإخفاء والتعديل الآمن للصور

عند نشر الصور، يُعد تعتيم وجوه المتظاهرين أو عناصر القمع أمراً إلزامياً لمنع التعرف عليهم. لكن الطرق التقليدية لا تعمل بكفاءة.



الفصل الثالث

التنظيف الجذري للأثر الرقمي

ملفاتك ليست مجرد صورة أو صوت؛ فهي تحمل "هوية رقمية خفية". كل صورة أو فيديو تسجله يحتوي تلقائياً على إحداثيات جغرافية دقيقة، وقت التسجيل، وطراز جهازك. في عقيدة المراقبة الذكية، لا تحتاج الشرطة لتتبعك إلى تحليل محتوى الفيلم؛ بل تقوم فقط بقراءة هذا "الأثر الخفي" واستخراج هويتك وموقعك. قبل نشر أي ملف، يجب تدمير هذه الروابط الرقمية بشكل جذري لكي لا تترك كاميرتك أي أثر لك.





3.1. العلامات الخفية الخطرة في الملفات (EXIF Data)

كل صورة تسجلها الهواتف الذكية تحتوي تلقائياً على هوية رقمية تسمى EXIF. تتضمن هذه الهوية المعلومات شديدة الأمان التالية:

- الإحداثيات الجغرافية الدقيقة لالتقاط الصورة (Geotagging) بناءً على GPS بدقة السنتيمتر.
- الوقت والتاريخ الدقيق لالتقاط الإطار (Timestamp).
- الطراز الدقيق للجهاز، الرقم التسلسلي لمستشعر الكاميرا، وإصدار نظام التشغيل.

إذا وصل هذا الملف بهذا الهيكل إلى شرطة فتا، فلن يحتاجوا إلى تحليل محتوى الصورة؛ بل ستكشف البيانات الوصفية (Metadata) مباشرة عن هوية المالك وموقعه الدقيق.

3.2. ورشة عمل عملية خطوة بخطوة لبرنامج Scrambled Exif (للأندرويد)

هذه الأداة هي تطبيق مفتوح المصدر بدون إعلانات ومجاني تماماً ومنعزل لإزالة البيانات الوصفية قبل مشاركة الملفات:

أ) قم بتنزيل وتثبيت تطبيق Scrambled Exif من المخازن الآمنة مثل (F-Droid).

ب) افتح التطبيق وفعل الخيارات التالية في قسم الإعدادات (Settings):

- تغيير اسم الملف إلى سلسلة أكواد عشوائية لحذف أثر التسمية (Pick random filename).
- إزالة بيانات نظام تحديد المواقع (Remove GPS Data) وإزالة بيانات الكاميرا (Remove Camera Data).

- **ج) الآن اذهب إلى معرض هاتفك، اختر الصورة الحساسة واضغط على زر المشاركة (Share).**
- **د) من بين التطبيقات، اختر Scrambled Exif؛ سيقوم البرنامج بتدمير البيانات الوصفية في أجزاء من الثانية ويفتح قائمة المشاركة الثانية.**

هـ) الآن قم بإرسال الملف المنظف عبر تطبيق مراسلة آمن.



3.3. ورشة عمل البيانات الوصفية لسطح المكتب باستخدام أداة ExifTool (ويندوز ولينوكس)

- أ) نظام تشغيل ويندوز بدون تثبيت أي برنامج: طريقة أبسط بكثير وبدون تنزيل برامج في ويندوز هي النقر بزر الماوس الأيمن على الصورة، النقر على خيار (Properties)، الانتقال إلى تبويب (Details) وفي أسفل النافذة النقر على العبارة (Remove Properties and Personal Information)، ثم اختيار الخيار الثاني وهو (Remove the following properties from this file)، تحديد كافة الخيارات والتأكيد.
- ب) للصحفيين الذين يعالجون حجماً كبيراً من الملفات على الكمبيوتر: تُعد أداة الطرفية ExifTool الخيار الأقوى. افتح الطرفية (Terminal) في لينوكس أو موجه الأوامر (Command Prompt) في ويندوز. للتنظيف الكامل وغير القابل للرجوع لكافة البيانات الوصفية الموجودة في مجلد يحتوي على مستندات وفيديوهات، اكتب الأمر التالي ونفذه:

```bash
exiftool -all= -overwrite_original /path/to/your/folder
```

(شرح المفاتيح: -all= تعني إزالة جميع العلامات، و -overwrite_original تعني الكتابة فوق الملف الأصلي دون حفظ نسخة احتياطية تحتوي على البيانات الوصفية).



الفصل الرابع

طرق التخزين الآمن والإخفاء السري للمعلومات

إذا تم مصادرة جهازك (هاتف أو حاسوب) في دوريات التفتيش في الشوارع، نقاط التفتيش، أو مداهمات المنازل، فإن الحذف البسيط للملفات أو حتى إعادة ضبط المصنع (Factory Reset أو Delete) لا يفيد شيئاً. الأجهزة الأمنية قادرة باستخدام الأجهزة وبرمجيات الاسترداد الجنائي (مثل أجهزة Cellebrite التي تنسخ الذاكرة الفيزيائية مباشرة) على استرداد الملفات حتى من شهور مضت. في هذه الظروف، الحل الوحيد للنجاة هو استخدام التشفير غير القابل للكسر، إخفاء البيانات (Steganography)، وأجهزة التدمير الذاتي.

4.1. ورشة عمل شاملة لبرنامج VeraCrypt

برنامج VeraCrypt هو المعيار الذهبي لتشفير سطح المكتب والذي يدعم عقيدة الإنكار القابل للتصديق؛ تتيح لك هذه التقنية بناء خزنة رقمية ذات طبقتين:

- هيكل الخزنة ذات الطبقتين:
  - **المجلد الخارجي (Outer Volume):** يفتح بكلمة مرور عادية. تضع في هذه الطبقة الملفات العادية والآمنة مثل المذكرات الجامعية أو الأفلام السينمائية.
  - **المجلد المخفي (Hidden Volume):** مخفي في قلب المجلد الخارجي. لا يُظهر هذا المجلد أي علامة على وجوده ويفتح بكلمة مرور قوية للغاية. يتم تخزين جميع مستندات وفيديوهات الاحتجاجات الخام ورخص المشروع هنا.
- **بروتوكول المواجهة في التحقيق:** إذا أُجبرت تحت ضغط أمني شديد على كشف كلمة المرور، فأعطِ المحقق كلمة مرور الطبقة الخارجية فقط؛ سيقوم النظام بفتح الطبقة الخارجية ويرى الضباط الملفات الآمنة. من الناحية الرياضية وخوارزميات التشفير، لا توجد طريقة يمكن للمحقق من خلالها إثبات وجود طبقة ثانية (مخفية) في تلك المساحة أيضاً؛ وجودها قابل للإنكار بالكامل.

4.2. حلول التشفير المتقدمة في منصة الهواتف المحمولة

بما أن VeraCrypt مخصص للكمبيوتر، يُنصح بالأدوات التالية لتنفيذ هندسة أمان على الهواتف الذكية:

- **تطبيق EDS NG لنظام أندرويد:** هذا البرنامج هو الأداة الأكثر اكتمالاً وقوة لمحاكاة معايير VeraCrypt على الجوال. يسمح لك EDS NG بفتح وإدارة الحاويات المشفرة (Volumes) التي أنشأتها على الكمبيوتر مباشرة على الهاتف، والحفاظ على نفس مستوى الأمان وخاصية "الإنكار القابل للتصديق" في الميدان.
- **تطبيق Cryptomator (التشفير القائم على الملفات):** بخلاف VeraCrypt الذي ينشئ خزنة متكاملة، يقوم Cryptomator بتشفير الملفات واحداً تلو الآخر. هذه الأداة حيوية للنشطاء الذين يضطرون لاستخدام المساحات السحابية الشائعة مثل Google Drive. يتم تشفير الملفات على الجوال قبل رفعها لكي لا تتمكن أي جهة وسيطة من الوصول إلى محتواها.

4.3. مفاتيح الموت والتدمير الطارئ (Panic Buttons)

في كثير من الأحيان يحدث الاعتقال في الشارع فجأة وليس لديك الوقت لمسح الملفات؛ هنا يجب أن تكون قد جهزت النظام لـ "التدمير الذاتي".

- **تطبيق Ripple (ريبل):** هو تطبيق مفتوح المصدر يعمل كـ "زر طوارئ". يمكنك ضبطه بحيث يؤدي الضغط على زر معين على الشاشة أو الضغط ثلاث مرات سريعة على زر التشغيل (Power) في الهاتف إلى قيام البرنامج تلقائياً بمسح تطبيقات المراسلة الحساسة، تسجيل الخروج من الحسابات، وتدمير ملفات محددة.
- **بروتوكول رمز مرور الخداع (Duress PIN):** تتيح لك بعض أنظمة التشغيل الآمنة تعيين رمز مرور كاذب؛ إذا طلب منك الضباط عند الاعتقال فتح قفل الهاتف وأدخلت رمز الخداع هذا، فلن يفتح الهاتف بل سيعود فوراً إلى إعدادات المصنع ويتم مسح جميع المعلومات بشكل لا رجعة فيه (Wipe).

4.4. النقل السريع إلى الأرشيف السحابي القائم على "المعرفة الصفرية"

هناك قانون ذهبي في توثيق الأزمات وهو أن جهازك المادي (الهاتف أو الكاميرا) يجب ألا يكون محلاً للاحتفاظ بالمعلومات لفترة طويلة. بمجرد تسجيل انتهاكات حقوق الإنسان والعودة إلى نقطة آمنة، يجب نقل الملفات إلى مساحة سحابية تستفيد من هندسة المعرفة الصفرية ثم تدميرها بالكامل من جهازك المادي. يُنصح باستخدام Proton Drive أو الإرسال المباشر عبر شبكة تور باستخدام منصة OnionShare. في هذه الخدمات، يتم تشفير الملفات قبل مغادرة جهازك باستخدام بروتوكول (E2EE)؛ حتى لو تم اختراق خوادم هذه الشركات، فلن يكون لديهم سوى مجموعة من الأكواد المشفرة لأن مفتاح فتح هذه الخزنة موجود في ذهنك وحدك.





5.1. هندسة الطبقات لشبكة البصل (Tor) وسكيوردراب (SecureDrop)

- لإرسال مستندات انتهاكات حقوق الإنسان إلى المنظمات الدولية، يجب ألا تستخدم أبداً المتصفحات العادية (Chrome أو Safari) لأن عنوان IP الخاص بك يُسجل في خوادم وسيطة. تمرر شبكة البصل (Tor) حركة المرور الخاصة بك عبر ثلاث طبقات من الخوادم العشوائية والمشفرة حول العالم (Relays)؛ الخادم الأول يعرف عنوان IP الخاص بك ولكنه لا يرى المحتوى، الخادم الثاني لا يعرف أي منهما، والخادم الثالث (Exit Node) يوصل المحتوى إلى الوجهة ولكنه لا يعرف المصدر الأساسي.
- سكيوردراب (SecureDrop) هي منصة مبنية على شبكة البصل (onion) تستخدمها وكالات حقوق الإنسان لتلقي المستندات من المسربين؛ من خلال الدخول إلى متصفح تور وإدخال عنوان SecureDrop المخصص للمؤسسة المستهدفة، يمكنك تحميل المستندات دون ترك أدنى أثر رقمي.

5.2. ورشة عمل تفعيل شبكة المِشّ غير المتصلة باستخدام Briar

في سيناريو ظلام الإنترنت الشامل (Internet Blackout) في الاحواز، يحافظ تطبيق المراسلة Briar على الشريان الاتصالي للنقاط الميدانية. هذا التطبيق لا يحتاج إلى خادم مركزي أو إنترنت، وينقل الرسائل عبر الواي فاي المحلي بدون إنترنت والبلوتوث بطريقة متسلسلة (Mesh Network) بين الهواتف.

- ملاحظة: يقوم نظام أندرويد بغلق تطبيقات الخلفية بشكل هجومي لتقليل استهلاك البطارية، مما يتسبب في قطع شبكة مِشّ Briar؛ لتطعيم التطبيق:
  a. اذهب إلى إعدادات الهاتف Settings > Apps > Briar.
  b. ادخل إلى قسم استهلاك بطارية التطبيق Battery > App Battery Usage.
  c. وغير وضع الاستهلاك من (Optimized) إلى (Unrestricted) بدون قيود.
  بهذا العمل يظل Briar مضاءً في الخلفية على مدار 24 ساعة ولن ينقطع برج الاتصال الخاص بك مع أعضاء الشبكة الآخرين.

5.3. بروتوكول تطعيم الحسابات بالكامل (Account Vaccination)

لمنع السيطرة على حسابات تيليجرام، واتساب، وشبكات التواصل الاجتماعي بعد مصادرة بطاقة SIM أو الاختراق الشبكي، فإن تطبيق خطوط الدفاع الثلاثة هذه إجباري:

- **إلغاء التحقق الثنائي عبر الرسائل القصيرة (SMS 2FA):** تعيد المشغلات الداخلية بناءً على طلب الأجهزة الأمنية إعادة بث رسائل التفعيل القصيرة (SMS Interception) بسهولة. لا تقم بتشغيل حساباتك بأرقام إيرانية، وأوقف دائماً التحقق الثنائي عبر الرسائل القصيرة في جميع الحسابات واضبطه حصرياً على تطبيقات توليد الرموز غير المتصلة مثل Google Authenticator أو Aegis.

- **تفعيل بروتوكول مفتاح المرور (Passkey) في حسابات جوجل وبروتون ميل:** فعّل ميزة Passkey؛ تستخدم هذه التقنية مستشعر بصمة الإصبع أو التعرف على الوجه المادي لهاتفك بدلاً من كلمة المرور لتسجيل الدخول إلى الحساب، وتجعل احتمال تسريب كلمة المرور أو التصيد الاحتيالي صفراً.

- **قطع الاتصال بجهات الاتصال (Contacts Sync):** في إعدادات الخصوصية لتيليجرام، جوجل، وإنستغرام، قم بإلغاء تفعيل خيار Sync Contacts واحذف جهات الاتصال المتزامنة مسبقاً (Delete Synced Contacts). يمنع هذا العمل خوارزميات القمع من رسم مخطط الاتصال الخاص بنقطتك عبر أرقام الهواتف المخزنة في الهواتف المصادرة.

ملاحظة: في عالم السيبراني الفزيائي، لا تصنع الأدوات معجزة وحدها؛ بل إن الانضباط التشغيلي والتكرار المستمر لهذه البروتوكولات هو ما يجعلك ناشطاً منيعاً. وعيك هو أعلى مستوى أمان لديك.



5.4. خدمة البريد الإلكتروني الآمن بروتون (ProtonMail)

تُعتبر رسائل البريد الإلكتروني التقليدية مثل Yahoo و Gmail بيئة غير آمنة للصحافة المواطنة وإرسال المستندات الحساسة في المناطق الخطرة؛ لأنها تحافظ على البيانات الوصفية بالكامل ومحتوى الرسائل متاح للمراقبة والمتابعة على الخوادم المركزية كنص عادي (Plain Text). تُعد خدمة ProtonMail ومقرها سويسرا المعيار الذهبي للمراسلات الآمنة والمبنية على هندسة "المعرفة الصفرية" (Zero-Knowledge) والتشفير من طرف لطرف (E2EE)، مما يعني أن شركة Proton نفسها غير قادرة على قراءة رسائلك.

بروتوكول التفعيل وإعداد حساب البريد الآمن:

a. **التسجيل بدون أثر:** عند إنشاء حساب في بروتون ميل، لا تستخدم أبداً رسائل البريد القديمة أو رقم هاتفك الشخصي للتحقق (Verification). لتجاوز حاجز التحقق، استخدم خيارات مثل الدفع بعملات رقمية مجهولة إذا كنت تشتري النسخة الممتازة، أو التحقق عبر اختبار الكابتشا (CAPTCHA) في بيئة شبكة تور (Tor).

b. **إعداد مفتاح المرور (Passkey):** كما ذكر في الأقسام السابقة، لتأمين الحساب ضد التصيد الاحتيالي والهجمات الإذاعية القائمة على بطاقة SIM، قم بإزالة كلمة المرور التقليدية وربط تسجيل الدخول إلى تطبيق بروتون بميزة البيومترية الهاتفية المادية الخاصة بك (Passkey).

التكتيكات المتقدمة عند إرسال المستندات الحساسة

- **آلية رسائل البريد الإلكتروني ذاتية التدمير (Self-Destructing Emails):** عند إرسال وثائق أو تقارير انتهاكات حقوق الإنسان إلى حسابات خارج بروتون أو حتى داخل الشبكة، وقبل النقر على زر الإرسال، انقر على أيقونة الساعة وحدد وقتاً لتدميرها (Expiration Time) (على سبيل المثال 24 أو 48 ساعة). بهذه الطريقة سيتم مسح البريد الإلكتروني تلقائياً وبشكل لا رجعة فيه من صندوق الوارد والمرسل بعد الوقت المحدد.
- **إرسال رسالة مشفرة لحسابات غير بروتون:** إذا اضطررت لإرسال وثيقة إلى بريد إلكتروني عادي مثل جيميل لمنظمة أو وسيلة إعلام، انقر على أيقونة القفل في أسفل قائمة الإرسال وضع كلمة مرور متفق عليها للبريد الإلكتروني. يتلقى المستلم رابطاً فقط ويجب عليه إدخال كلمة المرور لفتح ومحتوى البريد. بهذه الطريقة، لن ترى جدران الحماية للشبكة والتنصت الوسيط سوى رابط مشفر.
- **الحذف التلقائي للبيانات الوصفية للصور المرفقة:** يقوم بروتون ميل تلقائياً بتصفية بعض البيانات الوصفية الأساسية عند إرسال البريد الإلكتروني، ولكن وفقاً للانضباط التشغيلي لمشروع "الصوت الآمن"، يجب دائماً تنظيف الملفات أولاً عبر أدوات مثل Scrambled Exif أو ExifCleaner ثم إرفاقها بالبريد الإلكتروني



الخاتمة

الكتيب الذي تصفحته والبروتوكولات التي راجعتها ليست مجرد إرشادات لحماية البيانات؛ بل هذه الأدوات هي ستراتك الواقية في الحرب السيبرانية الخفية. في جغرافيا صعبة مثل إقليم الأهواز، كل صورة أو فيلم أو وثيقة تُسجل وتنقل عن انتهاكات حقوق الإنسان هي حجارة تسقط جدار الرقابة العالي والمقاطعة الإخبارية. عدسة كاميرتك هي نافذة نحو الحقيقة، ولإبقاء هذه النافذة مفتوحة، فإن بقاء الراوي خفياً هو أصل حيوي.

تذكر أن الأمن ليس وضعاً ثابتاً أو زراً للتشغيل؛ الأمن هو انضباط مستمر ويومي. الأدوات والتطبيقات والبروتوكولات المتقدمة مثل شبكة البصل، ObscuraCam، Briar، وVeraCrypt لا تصنع معجزة إلا إذا اقترنت بالوسواس التشغيلي والهدوء والتكرار الدائم. خطأ صغير واحد أو لحظة غفلة ناتجة عن الاستعجال في إرسال الخبر هي تلك الثغرة التي يتطلع إليها جهاز القمع للاختراق.

لقد تعلمنا في هذا الدليل كيف نجعل جدران الزنازين زجاجية، وكيف نخفي أثرنا الرقمي عن عيون خوارزميات شرطة فتا، وكيف يبقى شريان الاتصال للمجتمع المدني حياً في الظلام الدامس لانقطاع الإنترنت. ولكن فوق التكنولوجيا، فإن "التضامن، اليقظة، والوعي التقني الخاص بك" هو ما يجعل المقاومة منيعة. ابقَ مجهول الهوية، اعمل بمنعة، نظف التفاصيل بدقة جنائية (Forensic)، وتذكر أن النصر الأعظم في التوثيق هو رواية الحقيقة كاملة؛ بحيث يحيى الراوي حراً للروايات القادمة.



الصوت الآمن

Secure Voice

sv.khro.org

info@khro.org