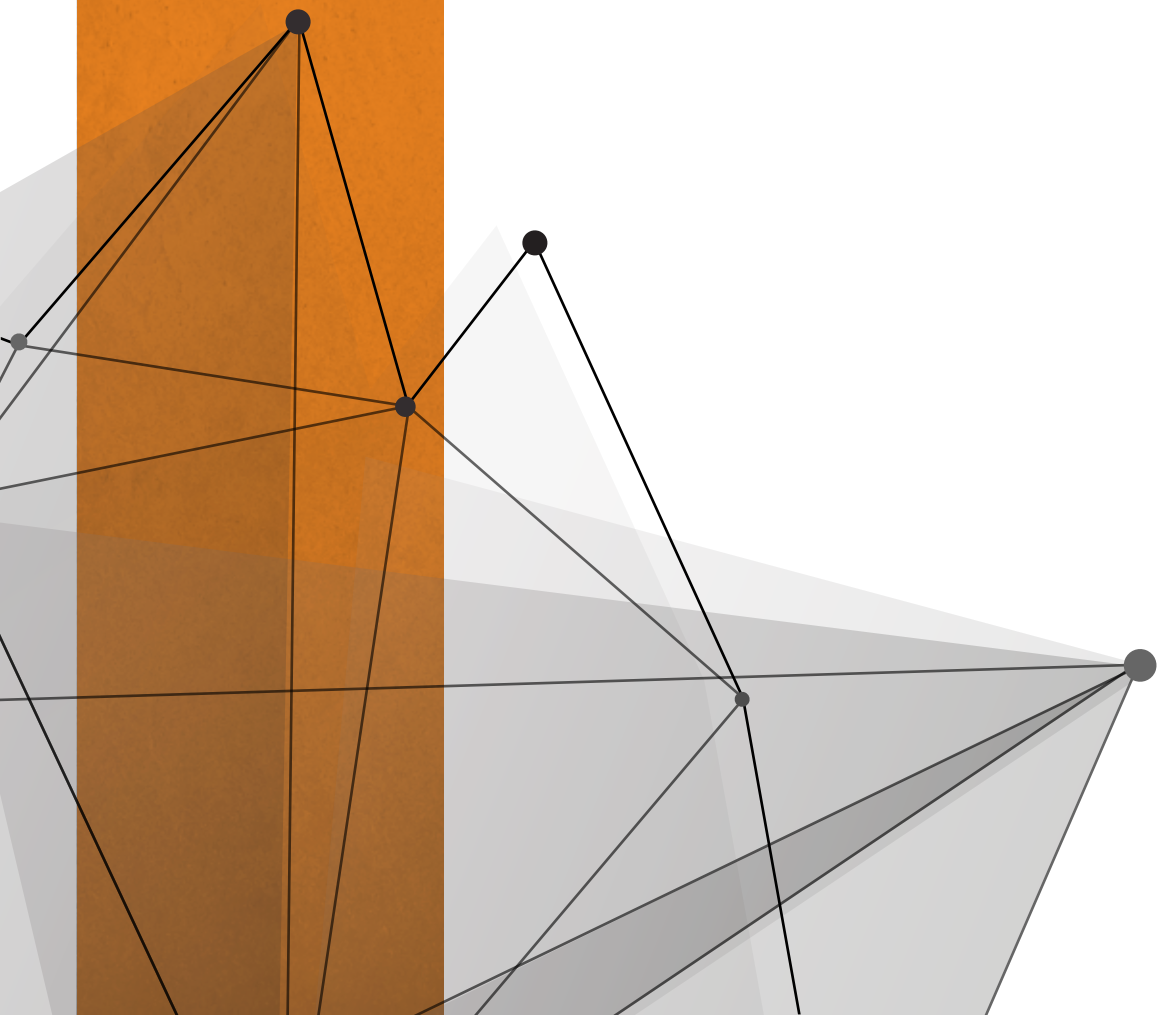
حجب مواقع الوِب في مصر

"التكتيكات والقوانين"



https://masaar.net

مسار - مجتمع التقنية والقانون

مايو ٢٠٢١

Masaar.net

خلفية

خلال الفترة السابقة أصدرت مسار - مجتمع التقنية والقانون، مجموعة من الإصدارات ذات الصلة بالرقابة على الإنترنت وحجب مواقع الوِب في مصر، والتي يمكن الوصول إليها عبر الروابط التالية:

- خط زمني لأحداث الرقابة على الإنترنت في مصر
- مواقع الوب المحجوبة في مصر
- حجب مواقع صحفية وحقوقية في مصر بمعدات "ساندفين"
- مُلخّص تحليلي /آخر الميادين.. رقابة ممنهجة على الإنترنت بدعوى حماية الأخلاق
- الرقابة على الإنترنت في زمن التباعد الاجتماعي

مُقدِّمة

يُركِّز هذا التقرير على ممارسة الرقابة على مواقع الوِب في مصر عن طريق الحجب، حيث يبدأ التقرير أولًا، بعرض البيئة القانونية ذات الصلة، بما يشمل إقرار القضاء المصري بسوابق قضائية تسمح بحجب المواقع، والقوانين التي تتضمن مواد تُتيح للسلطات ممارسة الحجب، مثل قانون مكافحة الإرهاب رقم ٩٤ لسنة ٢٠١٥، وقانون مكافحة جرائم تقنية المعلومات وقانون تنظيم الصحافة والإعلام.

يتناول القسم الثاني من التقرير شرحًا لتكنيكات حجب المواقع، مثل الحجب القائم على حجب عنوان بروتوكول الإنترنت (IP) وحزمة بروتوكولات الإنترنت (TCP/IP)، والحجب القائم على حجب نظام أسماء النطاقات (DNS)، والحجب القائم على الفحص العميق للحزم (Deep packet inspection)، واستخدام هذه التكنيكات التي تعتبر من أكثر الأساليب المُرتبطة بحجب مواقع الوِب في مصر، بالإضافة إلى شرح كيف تتم عملية (TCP rest attack) واستخدام الفحص العميق للحزم لحجب مواقع الوِب عبر (Reset Connection) كما يُقدِّم التقرير أيضًا سردًا لبعض أهم أحداث الرقابة على الإنترنت وحجب مواقع الوِب في مصر خلال السنوات الماضية.

أولًا : التطورات القانونية المُتعلقة بالحجب

تضع العديد من التشريعات والأحكام القضائية في مصر القواعد والمبادئ المُتعلّقة بفرض صور مختلفة للرقابة على المحتوى المرئي والمسموع والمقروء.

لم تكن هناك نصوص قانونية تُنظم عملية حجب مواقع الوِب قبل عام ٢٠١٥، لذلك بدأت ممارسة حجب مواقع الوِب باجتهادات قضائية واستخدام قوانين الاتصالات لتبرير الممارسة،

ثم تطور الأمر لإقرار بعض القواعد التي تسمح للجهات القضائية بتوقيع عملية الحجب، وفقًا لبعض الضوابط الاستثنائية مثل الحجب بموجب قانون مكافحة الإرهاب، إلا أن القواعد الاستثنائية لم تكن كافية لتطبيق عملية الحجب على نطاق واسع، فتجاوزت السلطات المصرية أزمات إقرار قوانين وبدأت في ممارسة عملية الحجب دون غطاء قانوني، ودون صدور قرارات رسمية معلنة، ومع مرور الوقت أصبح الحجب أمرًا طبيعيًا يواجهه المستخدمون بشكل يومي. لاحقًا، بدأت السلطات في إقرار عدد من التشريعات الأساسية واللوائح التنفيذية التي تُنظِّم عملية الحجب.

القضاء المصري يقر سوابق قضائية تسمح بالحجب

لم تكن ممارسات السلطة التنفيذية سببًا وحيدًا لترسيخ القواعد المُتعلِّقة بالحجب، حيث ساهمت الجهات القضائية بترسيخ هذه الممارسة، وذلك من خلال التفسير الخاطئ لنصوص القانون رقم (١٠) لسنة ٢٠٠٣ بإصدار قانون تنظيم الاتصالات، ومحاولة إيجاد مبرر قانوني يمكن من خلاله منع الوصول إلى المحتوى. خلال الفترة ما بين سنة ٢٠١١ حتى سنة ٢٠١٥، لم تكن هناك تشريعات تتحدث صراحة عن إمكانية الحجب أو توضح سلطة الجهات الإدارية وغيرها من جهات إنفاذ القانون في القيام بحجب مواقع الوِب.

في سنة ٢٠١٢ أقام أحد المحامين المصريين دعوى قضائية أمام محكمة القضاء الإداري يطالب فيها بإلزام الجهاز القومي لتنظيم الاتصالات ووزارة الاتصالات وتكنولوجيا المعلومات بحجب موقع يوتيوب وكافة الروابط التي تعرض ما عُرف بـ"الفيلم المُسيء للرسول" وجميع الروابط التي تعرض مقاطع مرئية "مناهضة للإسلام."

وبعد تداول الدعوى أصدرت محكمة القضاء الإداري حكمها، في ٢٠١٣، بحجب موقع يوتيوب لمدة شهر وحجب جميع الروابط التي تعرض الفيلم المسيء للرسول، واعتمدت الجهات القضائية المصرية تفسيرات خاطئة لنصوص المواد (٦٤) و (٦٧) من قانون تنظيم الاتصالات، استطاعت من خلالها أن تجد مسوغًا قانونيًا، يمكن من خلاله إلزام الجهات الإدارية بحجب المحتوى، من خلال التوسُّع في تفسير مفهوم الأمن القومي وضرورة حمايته.

تُلزم النصوص القانونية التي تم الاعتماد عليها من قانون تنظيم الاتصالات مُقدمي الخدمة بتوفير الإمكانيات الفنية من معدات ونظم وبرامج واتصالات داخل شبكة الاتصالات بحيث تتيح للقوات المسلحة وأجهزة الأمن القومي ممارسة اختصاصاتها، كما تسمح هذه النصوص لهذه الجهات الأمنية أن تخضع لإدارتها جميع خدمات وشبكات اتصالات أي مقدم خدمة في حالة حدوث كارثة طبيعية أو بيئية أو في الحالات التي تعلن فيها التعبئة العامة أو أية حالات أخرى تتعلق بالأمن القومي.

ولم تُحدِّد نصوص القانون طبيعة هذه الإمكانيات الفنية أو ضوابط استخدامها، كما لم يشمل القانون تعريفًا واضحًا لمفهوم الأمن القومي، لذلك توسعت المحكمة في تفسير هذا المفهوم الذي امتد ليشمل ما أُطلق عليه "الأمن القومي الاجتماعي" وضرورة حمايته ومنع ما قد يُشكِّل تهديدًا له، وانتهت المحكمة إلى سابقة قضائية تُلزم الجهات الإدارية باتخاذ إجراءات الحجب بموجب قانون تنظيم الاتصالات.

لذلك سعت المحاكم التي نظرت دعوى حجب اليوتيوب وروابط الفيلم المسيء إلى محاولة تعريف مفهوم الأمن القومي، حيث توسعت في تفسيره لترى أن عرض الفيلم المسيء يضر "الأمن القومي الاجتماعي" كما دعت المحكمة الإدارية العليا أثناء نظر الطعن على حكم اليوتيوب، إلى ضرورة سنِّ تشريع يمنع ويجرم كل بث - أيًا كانت وسيلته - من شأنه أن ينال من المعتقدات والثوابت الدينية للشعب المصري حفاظًا على السلام الاجتماعي ووحدة النسيج الوطني.

---

١ - نصوص قانون تنظيم الاتصالات ذات الصلة.

٢ - أحكام المحاكم المذكورة أعلاه.

٣ - المادة ٤٩ من القانون ٩٤ لسنة ٢٠١٥ بشأن مُكافحة الإرهاب "للنيابة العامة أو سلطة التحقيق المختصة، بحسب الأحوال، في الجرائم المنصوص عليها بالمواد (١٢، ١٥، ١٩، ٢٢) من هذا القانون، أن تصدر أمرًا مؤقتًا بغلق المقار، والأماكن، والمساكن، ومحال الإيواء على أن يصدر القرار من رئيس نيابة على الأقل، وتعتبر الأمتعة والأثاث المضبوط فيها في حكم الأشياء المحجوز عليها إداريًا بمجرد ضبطها حتى يفصل في الدعوى نهائيًا، وتسلم بعد جردها وإثباتها في محضر لحارس يكلف بحراسة الأختام الموضوعة على المقر أو المكان أو المحل أو المسكن المغلق، فإن لم توجد مضبوطات كلف بالحراسة على الأختام بالطريقة ذاتها، ويترتب على صدور الحكم بالبراءة سقوط أمر الغلق. وللنيابة العامة أو سلطة التحقيق المختصة وقف المواقع المنصوص عليها

قانون مُكافحة الإرهاب يُنظم عملية الحجب لأول مرة

في٢٠١٥، صدر قانون مكافحة الإرهاب، الذي نظم لأول مرة عملية حجب المواقع حيث أعطى القانون صلاحية للنيابة العامة أو سلطة التحقيق المختصة بوقف المواقع أو حجبها، وذلك إذا كان الموقع قد "أُنشئ بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية أو لبث ما يهدف إلى تضليل السلطات الأمنية أو التأثير على سير العدالة في شأن أية جريمة إرهابية أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج."

التوسع في ممارسة الحجب دون مُبرِّر قانوني

خلال الأعوام الأربعة الأخيرة تزايدت الممارسات المتعلقة بحجب مواقع الوِب، ولم تُعلن أي جهة رسمية مسؤوليتها عن هذه الممارسات، حيث لم يكن هناك قرار مُعلن يمكن من خلاله قراءة مدى قانونية هذه الممارسات أو الرقابة على مدى مشروعيتها، هذا النمط الشائع من الممارسات يهدف - في الغالب - إلى ترسيخ إجراءات غير قانونية بهدف تهيئة الرأي العام لقبولها تدريجيًا، ومن ثم تسهيل تقنين هذه المُمارسات من خلال إقرار قواعد قانونية، غير دستورية، من شأنها أن تفرض قيودًا على الحقوق والحريات الأساسية.

حيث بدأت السلطات المصرية في استخدام الحجب بشكل منهجي في مايو ٢٠١٧، فحجبت السلطات ما يقرب من ٢٢ موقع وِب، وتوسعت في تطبيق الحجب بشكل كبير.

٤- المادة ٢٩ من القانون ٩٤ لسنة ٢٠١٥ بشأن مُكافحة الإرهاب "يُعاقب بالسجن المشدد مدة لا تقل عن خمس سنين، كل من أنشأ أو استخدم موقعًا على شبكات الاتصالات أو شبكة المعلومات الدولية أو غيرها، بغرض الترويج للأفكار أو المعتقدات الداعية إلى ارتكاب أعمال إرهابية، أو لبث ما يهدف إلى تضليل السلطات الأمنية، أو التأثير على سير العدالة في شأن أية جريمة إرهابية، أو لتبادل الرسائل وإصدار التكليفات بين الجماعات الإرهابية أو المنتمين إليها، أو المعلومات المتعلقة بأعمال أو تحركات الإرهابيين أو الجماعات الإرهابية في الداخل والخارج. ويُعاقب بالسجن المشدد مدة لا تقل عن عشر سنين، كل من دخل بغير حق أو بطريقة غير مشروعة موقعًا إلكترونيًا تابعًا لأية جهة حكومية، بقصد الحصول على البيانات أو المعلومات الموجودة عليها أو الاطلاع عليها أو تغييرها، أو محوها أو إتلافها أو تزوير محتواها الموجود بها، وذلك كله بغرض ارتكاب جريمة من الجرائم المشار إليها بالفقرة الأولى من هذه المادة أو الإعداد لها".

تضمين الحجب كقاعدة أساسية في التشريعات الجديدة

استطاعت السلطات تقنين الممارسات التي بدأت في ٢٠١٧، عبر دمج حجب مواقع الوِب في العديد من التشريعات، حيث نُصّ على الحجب في تشريعات تنظيمية وأخرى جزائية تحت توصيفات قانونية مختلفة. ومن أمثلة هذه التشريعات قانون مُكافحة جرائم تقنية المعلومات وقانون تنظيم الإعلام والصحافة.

أ. الحجب كتدبير إجرائي لحماية الأمن القومي في قانون مُكافحة جرائم تقنية المعلومات

صدر قانون الجريمة الإلكترونية رقم ١٧٥ لسنة ٢٠١٨ في أغسطس من سنة ٢٠١٨ ليُنظِّم الحالات التي يمكن تطبيق الحجب خلالها كتدبير أولي، يُعطي القانون صلاحية لجهات التحقيق لإصدار قرار بحجب مواقع الوِب متى رأت أن المحتوى المنشور على هذه المواقع يُشكّل جريمة أو تهديدًا للأمن القومي أو يُعَرِّض أمن البلاد أو اقتصادها القومي للخطر، كما يعطي القانون صلاحية للجهات الشُرطيّة في حال الاستعجال والضرورة بطلب حجب مواقع الوِب قبل استصدار حكم قضائي. وتكون صلاحية اتخاذ إجراءات الحجب قائمة، متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات، أو أرقام، أو صور، أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدًا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر.

---

٥ - المادة ٧ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مُكافحة جرائم تقنية المعلومات:

لجهة التحقيق المختصة متى قامت أدلة على قيام موقع يبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية أو ما في حكمها، بما يعد جريمة من الجرائم المنصوص عليها في هذا القانون، ويشكل تهديدًا للأمن القومي أو يعرض أمن البلاد أو اقتصادها القومي للخطر، أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيًا.

وعلى جهة التحقيق عرض أمر الحجب على المحكمة المختصة، منعقدة في غرفة المشورة خلال أربع وعشرين ساعة مشفوعًا بمذكرة برأيها. وتصدر المحكمة قرارها في الأمر مسببًا إما بالقبول أو بالرفض، في مدة لا تجاوز اثنتين وسبعين ساعة من وقت عرضه عليها.

ويجوز في حالة الاستعجال لوجود خطر حال، أو ضرر وشيك الوقوع، أن تقوم جهات التحري والضبط المختصة بإبلاغ الجهاز، ليقوم بإخطار مقدم الخدمة على الفور بالحجب المؤقت للموقع أو المحتوى أو المواقع أو الروابط المذكورة في الفقرة الأولى من هذه المادة وفقًا لأحكامها. ويلتزم مقدم الخدمة بتنفيذ مضمون الإخطار فور وروده إليه.

ب. الحجب كعقوبة إدارية في قانون تنظيم الصحافة والإعلام ولوائحه التنفيذية

صدر قانون تنظيم الإعلام والصحافة رقم ١٨٠ لسنة ٢٠١٨ ليُعطي صلاحيات واسعة للمجلس الأعلى لتنظيم الإعلام تسمح له بفرض أشكال مختلفة من الرقابة على مواقع الوِب والصفحات الشخصية، حيث أعطت المادة ٩١ من القانون صلاحية للمجلس باتخاذ الإجراء المناسب حيال المخالفة وله في سبيل ذلك: وقف أو حجب الموقع أو المدونة أو الحساب في حال قيام الموقع أو الحساب بنشر أو بث أخبار كاذبة أو ما يدعو أو يحرض على مخالفة القانون أو إلى العنف أو الكراهية، أو ينطوي على تمييز بين المواطنين، أو يدعو للعنصرية، أو التعصب أو يتضمن طعنًا في أعراض الأفراد أو سبًّا أو قذفًا لهم أو امتهانًا للأديان السماوية أو للعقائد الدينية.

كما أقرت اللائحة التنفيذية لقانون تنظيم الإعلام والصحافة ولائحة الجزاءات التي أقرها المجلس الأعلى لتنظيم الإعلام والصحافة، الضوابط المُتعلقة بحجب المواقع والحسابات الخاصة على مواقع التواصل الاجتماعي.

---

٦ - وعلى جهة التحري والضبط التي قامت بالإبلاغ أن تحرر محضرًا تثبت فيه ما تم من إجراءات وفق أحكام الفقرة السابقة يعرض على جهات التحقيق خلال ثمان وأربعين ساعة من تاريخ الإبلاغ الذي وجهته للجهاز، وتتبع في هذا المحضر ذات الإجراءات المبينة بالفقرة الثانية من هذه المادة، وتصدر المحكمة المختصة قرارها في هذه الحالة إما بتأييد ما تم من إجراءات حجب، أو بوقفها.

فإذا لم يعرض المحضر المشار إليه في الفقرة السابقة في الموعد المحدد، يعد الحجب الذي تم كأن لم يكن.

ولمحكمة الموضوع أثناء نظر الدعوى، أو بناء على طلب جهة التحقيق أو الجهاز أو ذوي الشأن أن تأمر بإنهاء القرار الصادر بالحجب، أو تعديل نطاقه.

وفي جميع الأحوال، يسقط القرار الصادر بالحجب بصدور أمر بألا وجه لإقامة الدعوى الجنائية، أو بصدور حكم نهائي فيها بالبراءة.

نبذة عن المجلس الأعلى ودوره.

٧ - المادة ٩١ : يحظر على الصحيفة أو الوسيلة الإعلامية أو الموقع الإلكتروني، نشر أو بث أخبار كاذبة أو ما يدعو أو يحرض على مخالفة القانون أو إلى العنف أو الكراهية، أو ينطوى على تمييز بين المواطنين أو يدعو إلى العنصرية أو التعصب أو يتضمن طعنًا في أعراض الأفراد أو سبًا أو قذفًا لهم أو امتهانا للأديان السماوية أو للعقائد الدينية.

واستثناء من حكم المادة الأولى من مواد إصدار هذا القانون، يلتزم بأحكام هذه المادة كل موقع إلكتروني شخصي أو مدونة إلكترونية شخصية أو حساب إلكتروني شخصي يبلغ عدد متابعيه خمسة آلاف متابع أو أكثر.

ومع عدم الإخلال بالمسؤولية القانونية المترتبة على مخالفة أحكام هذه المادة يجب على المجلس الأعلى اتخاذ الإجراء المناسب حيال المخالفة وله في

ثانيًا: تكنيكات حجب مواقع الوِب في مصر

يُقدِّم هذا القسم شرحًا تقنيًا لتكنيكات حجب المواقع الأكثر انتشارًا في مصر، وقد اعتمدنا في هذا الجزء من هذا التقرير على:

ـ القياسات الخاصة بمصر التي تُنشر على موقع OONI Explore ، التي جُمعت بواسطة برمجية (Probe-CLI) وقائمة النطاقات التي يُطورها Citizen Lab و OONI، التي قامت مسار - مجتمع التقنية والقانون، بالمساهمة في تطويرها خلال الأشهر السابقة.

ـ التقارير التي صدرت عن مسار والمنظمات المحلية والدولية المهتمة بوضع حرية الإنترنت في مصر محليًا ودوليًا.

ـ أدوات تساعد في إجراء اختبارات TCP connection لمواقع الوِب وعناوين بروتوكولات الإنترنت وحجبها، مثل: Telnet وCurl وNC.

ـ أدوات تساعد في عمل Reverse DNS lookup بهدف التدقيق في نظام أسماء النطاقات (DNS)، مثل: nslookup وDig و Host.

١. كيف يتم الحجب القائم على حجب عنوان IP وبروتوكول TCP/IP

يحمل كل جهاز - مُتّصل بأي شبكة - عنوان بروتوكول الإنترنت (IP Address) والذي يعمل كمُعرِّف رقمي للجهاز، يُمكِن أن يكون هذا الجهاز حاسوبًا، أو طابعة، أو هاتفًا محمولًا أو أي جهاز آخر مُتّصل بشبكة الإنترنت أو بأي شبكة تستخدم بروتوكول (TCP/IP).

يوجد نوعان من بروتوكول (TCP/IP)، الأول هو الإصدار الرابع، وهو الأكثر شيوعًا، ويتكون من ٣٢ بت، ويكتب على شكل أرقام يفصل بين كل رقمين نقطة (.)، والثاني هو الإصدار السادس ويتكون من ١٢٨ بت ويُكتب على شكل مجموعات يفصل بينها الرمز(.).

يُعتبر بروتوكول التحكم بالنقل (TCP) أحد البروتوكولات الأساسيّة في حزمة بروتوكولات الإنترنت، فهو المسؤول عن نقل البيانات بين جهازين أو أكثر متصلين بشبكة الإنترنت، وتعتمد تطبيقات الإنترنت الرئيسية (على سبيل المثال خدمات البريد الإلكتروني ومواقع الوِب وخدمات نقل الملفات) على هذا البروتوكول.

كل نطاق لموقع وِب على الإنترنت يحمل عنوان بروتوكول إنترنت (IP Address)، يُشير إلى الخادوم المُستضاف عليه موقع الوِب، على سبيل المثال النطاق (masaar.net) يحمل عنوان بروتوكول إنترنت (١٠٤,٢١,٧٨,٨٦)، وعندما يقوم المستخدم باستخدام متصفح الإنترنت لتصفُّح موقع (masaar.net) فإن مُتصفِّح الإنترنت يقوم بالبحث عن عنوان بروتوكول الإنترنت المقابل للنطاق الذي يُريد المُستخدِم تصفُّحه، وتتم هذه العملية عبر نظام أسماء النطاقات (Domain Name System) وهو النظام المسؤول عن تخزين المعلومات المُتعلّقة بأسماء نطاقات الإنترنت (Domain Names) في قاعدة بيانات تحتوي على البيانات اللازمة لربط عناوين بروتوكولات الإنترنت بأسماء النطاقات المختلفة.

يُمكن للجهات المسؤولة عن إدارة وتشغيل الاتصالات ومُقدمي خدمات الإنترنت أن تحجب مواقع الوِب عبر حجب عنوان بروتوكول الإنترنت وحزمة بروتوكولات الإنترنت، بحيث يتم منع تدفق البيانات من وإلى عنوان بروتوكول إنترنت مُعيّن أو منفذ مُعيّن(Port).

المنفذ هو رقم مُلحق ببروتوكول الإنترنت يُستخدم لتمييز الخدمات المختلفة الموجودة على نفس الخادوم بحيث يمكن لهذا الخادوم تقديم أكثر من خدمة.

في حالة حجب موقع وِب عبر حجب عنوان بروتوكول الإنترنت وحزمة بروتوكولات الإنترنت، عند طلب المُستخدم تصفُّح موقع وِب معين، فإن مُقدِّم خدمة الإنترنت يحظر وصول المستخدمين إلى عنوان بروتوكول إنترنت مُعين، ويُمكن أن يحظر مُقدّم خدمة الإنترنت استخدام منفذ مُعيّن بهدف منع خدمة مُعيّنة مثل خدمات الشبكات الافتراضية (VPN) على سبيل المثال.

يُعتبر الحجب القائم على حجب عنوان بروتوكول الإنترنت (IP Address) وبروتوكول (TCP/IP) ضعيف نسبيًا، حيث يُمكن للمواقع/الخدمات التي تتعرّض للحجب عبر هذه الطريقة تغيير عنوان بروتوكول الإنترنت بسهولة، كما أن انتشار خدمات شبكات توصيل المحتوى (content delivery network) يُبطل فاعلية هذا النوع من الحجب.

شبكات توصيل المحتوى عبارة عن مجموعة من الخواديم المُوزّعة في أماكن جغرافية مختلفة وتحتوي على نُسخ من مواقع الوِب، بحيث عندما يطلب مستخدم في منطقة جغرافية مُعيّنة تصفح موقع يستخدم هذه الميزة فإن شبكة توصيل المحتوى تُرسله إلى أقرب خادوم بحيث يكون التصفح سريعًا.

٢. الحجب القائم على حجب نظام أسماء النطاقات (DNS)

كما ذكرنا فإن نظام أسماء النطاقات (DNS) عبارة عن قاعدة بيانات تُخزِّن المعلومات التي تتعلق بأسماء النطاقات بحيث يمكن الربط بين عنوان بروتوكول الإنترنت واسم النطاق، قاعدة البيانات هذه تُخزّن على خواديم مركزية تُسمى (Root name servers) تحتوي على قاعدة البيانات الكاملة لأسماء النطاقات وعناوين بروتوكول الإنترنت الخاص بها. كما يستخدم مقدمو خدمة الإنترنت خواديم تخزين مؤقّتة (Recursive DNS Servers) لنظام أسماء النطاقات تحتوي على نسخة من قاعدة بيانات نظام أسماء النطاق، وذلك لتحسين كفاءة وسرعة عملية البحث عن أسماء النطاقات.

وعندما يطلب المستخدم من مُتصفِّح الإنترنت الوصول إلى اسم نطاق موقع وِب مُعيّن (masaar.net) على سبيل المثال، فإن المُتصفّح يطلب من خادوم (Resolver) أن يقوم - بالنيابة عن المستخدم- بإرسال استفسارات حول المعلومات الموجودة في نظام أسماء النطاقات وإرسالها إلى جهاز المستخدم، وهذه الاستفسارات هي التي ينتج عنها ترجمة أسماء النطاقات إلى عنوان بروتوكول الإنترنت.

عندما يستخدم مُقدِّم خدمة الإنترنت تكنيك الحجب القائم على حجب نظام أسماء النطاقات، فإن خادوم (Resolver) سيتحقق مما إذا كان موقع الوِب المطلوب من قبل المستخدم محظورًا أم لا، وعندما يطلب المُستخدم دخول موقع وِب محجوب فإن خادوم (Resolver) يُرجع معلومات غير صحيحة وبالتالي لا يمكن إتمام عملية وصول المُستخدم لموقع الوِب.

٣. الحجب القائم على الفحص العميق للحزم (Deep packet inspection)

الفحص العميق للحزم (Deep packet inspection) هو تقنية متطورة يمكن استخدامها من قبل مُقدِّمي خدمة الإنترنت لفحص محتوى حزم البيانات وإدارة حركة مرورها على الشبكة. وعندما يستخدم مُقدِّمي خدمة الإنترنت الحجب القائم على الفحص العميق للحزم فإن مُقدِّمي الخدمة سيكون لهم القدرة على رؤية حركة مرور البيانات بين المستخدم وخواديم الإنترنت عبر أجهزة حواسيب مُعدّة لذلك، بحيث تمنع وصول المُستخدم لأحد مواقع الوِب أو خدمات مُعيّنة مثل خدمات الاتصالات الصوتية على الإنترنت (Voip) ولا تكون هذه التقنية فعّالة في الحجب إذا كان الاتصال مُعمَّى بالكامل.

أ. بروتوكول نقل النص التشعُّبي الآمن (HTTPS)

يوجد العديد من البروتوكولات التي يعتمد عليها الإنترنت في نقل البيانات مثل: (HTTP, FTP, VoIP) وقد اعتمد الوِب في بدايته على بروتوكول نقل النص التشعُّبي (HTTP) لنقل صفحات مواقع الوِب.

يعمل بروتوكول نقل النص التشعُّبي عبر مجموعة إجراءات يقوم بها مُتصفِّح الإنترنت بحيث يقوم بإرسال طلب المستخدم إلى الخادوم، الذي يقوم بدوره بالرد على طلب المُتصفِّح بالمحتوى المطلوب ومن ثم يستقبل المُستخدم المحتوى المطلوب.

لا يوفِّر بروتوكول نقل النص التشعُّبي (HTTP) تشفيرًا أثناء نقل البيانات بين المستخدم والخادوم، لذلك تم تطوير بروتوكول طبقة المنافذ الآمنة (Secure Socket Layer-SSL) والذي يعمل بالتزامن مع بروتوكول نقل النص التشعُّبي (HTTP) بحيث يقوم بمهمة تأمين البيانات خلال حركتها بين الأطراف المختلفة على شبكة الإنترنت، فيُشفِّر كافة الاتصالات دون تدخل من المُستخدم أثناء استخدامه لأيٍّ من خدمات الإنترنت التي تستخدم بروتوكول طبقة المنافذ الآمنة (SSL).

لاحقًا تم تقديم بروتوكول (Transport Layer Security- TLS) ليخلف بروتوكول (Secure Socket Layer-SSL) كبروتوكول تشفير معياري يمكن استخدامه وتركيبه على بروتوكولات نقل بيانات موجودة بالفعل مثل (HTTP, FTP):

الاستخدام الأكثر شيوعًا - والمعني في سياق هذا التقرير - هو استخدام بروتوكول (TLS/SSL) مع بروتوكول نقل النص التشعبي (HTTP) المُستخدم في الوصول إلى صفحات الإنترنت لتقديم إصدار أكثر أمانًا ومُشفّر وهو ما يُعرف ببروتوكول: (Hypertext Transfer Protocol Secure-HTTPS)، ويُمكن للمستخدم ملاحظة ما إذا كان موقع وِب يعتمد على هذا البروتوكول أم لا عبر فحص عنوان الموقع، فإن كان يبدأ بـ(HTTPS) فهو يستخدم البروتوكول وإن كان يبدأ بـ(HTTP) فهو لا يستخدمه.

كيف يعمل بروتوكول (HTTPS) ؟

للقيام بعملية تشفير الاتصال بين الخادوم والمستخدم، يستخدم بروتوكول(SSL/TLS) خوارزمية تعتمد على توليد زوج من المفاتيح،أحدهما عمومي (Public Key) والثاني خاص (Private Key) ويتم توليدهما بحيث يكون كل مفتاح فريد لا يمكن تكراره.

يمكن لأي طرف أن يُرسل بيانات مُشفّرة باستخدام المفتاح العمومي ولا يمكن فك تشفير هذه البيانات إلا باستخدام المفتاح الخاص المرتبط بالمفتاح العمومي.

وللقيام بعملية التشفير وفك التشفير، يستخدم بروتوكول (SSL/TLS) شهادة استيثاق (Public key Certificate) تَربِط زوج مفاتيح التشفير بهويات مواقع الوِب، بحيث يُمكن إجراء عملية تُسمى التوقيع (Digital Signature) يتم خلالها الاستيثاق من هوية مواقع الإنترنت لمنع انتحال أي خادم لهوية خادم آخر بهدف خداع المستخدم. وتحتوي الشهادات على المفتاح العمومي وتوقيع إلكتروني ومعلومات عن كلٍّ من الهوية المرتبطة بالشهادة وجهة إصدارها (Certificate Authority). هناك العديد من الجهات التي تُصدر الشهادات الرقمية (Certificate Authorities) هذه الجهات تُصدر الشهادات الرقمية لتُستَخدم من قبل أطراف ثالثة (أصحاب مواقع الوِب على سبيل المثال) بحيث تكون الجهة المُصدرة للشهادة ضامنة أن المفتاح العمومي المُتضمن بداخلها مملوك لمؤسسة أو موقع مُعيّن. وإذا تم توقيع شهادة مُقدّمة من موقع وِب يستخدم بروتوكول (HTTPS) من قِبل جهة (Certificate Authority) موثوق بها لإصدار الشهادات الرقمية، فيمكن للمستخدمين التأكد من أن هوية الموقع قد تم التحقق منها من قبل طرف ثالث موثوق به ومدقق.

كيف يتم استخدام الفحص العميق للحزم في حجب مواقع الوِب في مصر

بشكل عام يعتمد هذا التكنيك على توظيف تقنية الفحص العميق للحزم لاعتراض أكبر كَمٍّ من حركة مرور البيانات (غير المُشفّرة) عبر الشبكة، ومن ثم تحليلها واستخراج معلومات منها مثل البروتوكول المستخدم ووجهة الاتصال والإشارة إلى اسم الخادوم (Server Name Indication-SNI) وهي التي تحتوي على قيمة تُشير إلى اسم النطاق الذي يحاول العميل (المستخدم) الوصول إليه.

كشف موقع الوِب المطلوب حجبه

في بداية إنشاء الاتصال بين الخادم والعميل (مُتصفِّح الإنترنت)، يتم إجراء عملية تُسمى المصافحة (Handshake) وهي المسؤولة عن وضع القواعد التي سيتم الاعتماد عليها للاتصال بين الخادوم والعميل (المُتصفّح) قبل بدء الاتصال، بحيث تُرسل بعض البيانات الوصفية في صورة غير مشفرة (Plain/text)، من ضمنها الإشارة إلى اسم الخادوم (Server Name Indication-SNI) والذي يحمل اسم النطاق المطلوب الوصول إليه. وتكمن أهمية الإشارة إلى اسم الخادوم (Server Name Indication-SNI) في ضمان إرسال الخادوم للشهادة الخاصة باسم النطاق المطلوب الوصول إليه، خاصة في حالة استضافة مواقع ونطاقات أخرى على نفس الخادوم.

لاعتبارات متعددة، أهمها طبيعة البنية التحتية التي تدعم أهم التطبيقات والخدمات على الإنترنت، على سبيل المثال خدمات الحوسبة السحابية (Cloud Computing) مثل: (Google Cloud Platform) و(AWS) يكون الإشارة إلى اسم الخادوم (Server Name Indication-SNI) عامل أساسي يعتمد عليه نجاح الاتصال ببروتكول (HTTPS) ليُحدِّد مفاتيح التشفير المطلوبة لنجاح الاتصال.

يُمثِّل الإشارة إلى اسم الخادوم (Server Name Indication-SNI) هدفًا رئيسيًا لعمليات الرقابة والحجب التي تعتمد على الفحص العميق للحزم (Deep packet inspection)، بحيث يتم استخدامه للتعرف على الاتصال بين خادوم مُعين والعميل (المُستخدمون) ومن ثم، يتم إفشال الاتصال بينهما عبر استخدام TCP reset injection.

كيف يتم استخدام TCP reset injection لإفشال الاتصال؟

كما تناولنا في العناوين السابقة بروتوكول التحكم بالنقل (TCP) وهو البروتوكول الذي يتحكم وينظم حركة البيانات خلال الشبكة في صورة حزم (packets) وبيانات وصفية بين الخادم (Server) والعميل(Client)، كما يضمن بروتوكول (TCP) التأكد من وصول حزم البيانات خلال الاتصال بشكل سليم وإعادة إرسال أي بيانات مفقودة أو وصلات تالفة (Corrupted).

كل حزمة بيانات تتضمن مجموعة من الترويسات والأعلام (Headers/Flags)، تستخدم الترويسات والأعلام في تنظيم حركة البيانات بين أطراف الاتصال في سيناريوهات مختلفة.

تتضمن الأعلام (Flags) الموجودة في كل حزمة بيانات علمًا يسمى: (RST flag) في الظروف العادية يتم استخدام هذا العلم في إعلام أحد أطراف الاتصال بوجود مشكلة لدى الطرف الآخر بحيث لا يمكنه الاستمرار في إرسال/استقبال بيانات.

في معظم حركات مرور الحزم (Web Traffic)، يتم تعيين قيمة ٠ لـ (RST flag) ولا يكون لهذه القيمة أي تأثير، وإذا تم تعيينه القيمة ١، فإن ذلك يُشير إلى أن اتصال (TCP) يجب أن يتوقف فورًا.

عند استخدام (TCP reset attack) بهدف حجب مواقع الوِب، فإن مُقدِّم خدمة الإنترنت يقوم بهجوم بهدف حقن بيانات وصفية مزورة تحتوي على (RST flag) يحمل قيمة ١ بدلًا من ٠، ما يتسبب في إنهاء الاتصال من أحد أطرافه واعتباره اتصالًا فاشلًا.

ثالثًا: استمرار السلطات المصرية في الحجب

يتناول هذا القسم من التقرير بعض وقائع الرقابة على الإنترنت وحجب مواقع الوِب، التي تم التأكُّد منها خلال الفترة السابقة.

اكتشاف Middle Boxes في بعض الحالات

في سبتمبر٢٠١٩، اندلعت مظاهرات في مصر، وألقت السلطات المصرية القبض على عدد ضخم من المتظاهرين بالإضافة إلى حالات قبض عشوائي متعددة، وعلى أثر هذه التظاهرات قامت السلطات المصرية بممارسة حجب مواقع الوِب وتطبيقات التراسل الفوري.

حجب قناة الحرة وبي بي سي

أشار تقرير صادر عن OONI، أن السلطات المصرية قد حجبت موقع قناة الحرة وموقع بي بي سي في سبتمبر ٢٠١٩، وقد وجد التقرير أن العديد من القياسات التي جُمعت من مصر عن موقع بي بي سي قد أظهرت أخطاء TLS على شبكة الشركة المصرية للاتصالات (AS8452) وشبكة شركة أورانج مصر (AS37069) كما أظهرت القياسات الأخرى التي جُمعت من شركة فودافون مصر (AS36935) خطأ Timeout Error عند محاولة الحصول على محتوى الموقع. كما أظهرت القياسات أيضًا مؤشرًا قويًا على وجود شكل من أشكال تقنية فحص الحزم العميقة (DPI) التي تتعامل مع TLS والتي من المرجح أن تكون بصمة حقل SNI الخاص بمصافحة TLS.

أيضًا أوضحت القياسات التي جُمعت من قبل "مسار" من مصر إلى أن موقع قناة الحرة قد تعرّض للحجب في مصر، كما لوحظت هذه الحالات على شبكتين تم اختبارهما: فودافون مصر (AS36935) والمصرية للاتصالات (AS8452) وتُشير القياسات التي جُمعت خلال سبتمبر ٢٠١٩ من مصر إلى أن مزودي خدمة الإنترنت المصريين يعيدون ضبط الاتصالات (reset connection) من خلال استخدام معدات الفحص الدقيق للحزم (DPI).

حجب تطبيقات التراسل الفوري

أظهرت القياسات التي جُمعت في سبتمبر ٢٠١٩، أن السلطات المصرية قد حاولت حجب مواقع الوِب الخاصة بتطبيقات التراسل الفوري الشهيرة، خاصة التي تُقدِّم ميزة التعمية. وقد رُصد حجب ١٤ موقعًا من مواقع تطبيقات التراسل الفوري الشهيرة:

- على شبكة فودافون: wickr.com و signal.org وwire.com
- على شبكة وي: wechat.com و line.me و surespot.me و pryvatenow.com و skype.com و icq.com و groupme.com و kik.com و voxer.com و zello.com و trillian.im

وبالتدقيق في قياسات متعلِّقة بموقع الوِب الخاص بتطبيق واير والنطاقات التي يستخدمها التطبيق لتشغيل خدماته، فقد وُجد أن التطبيق يستخدم النطاقات التالية:

- https://prod-nginz-https.wire.com
- https://prod-nginz-ssl.wire.com
- https://prod-assets.wire.com
- https://wire-app.wire.com
- https://clientblacklist.wire.com

وقد أظهرت القياسات التي جُمعت من شبكة فودافون أن النطاقات سابقة الذكر قد حُجبت. كما حُجبت أيضًا مجموعة أخرى من النطاقات الفرعية لموقع Wire.com:

- https://pwa.wire.com
- https://wire-docs.wire.com
- https://services.wire.com
- https://teams.wire.com
- https://support.wire.com

إعاقة الوصول لتويتر

في شهر سبتمبر 2019، أبلغ العديد من المستخدمين المصريين عن عدم قدرتهم على استخدام تطبيق تويتر على الهواتف المحمولة من خلال الإنترنت المحمول (4g/3g)، ويُرجّح أن تكون السلطات المصرية قد حاولت حجب تويتر على شبكة فودافون أو على الأقل كانت محاولة لخنق الوصول لتويتر (throttling).

بتجربة تطبيق تويتر على أندرويد وُجد أنه يستخدم عناوين بروتوكول الإنترنت التالية:

- 104.244.42.1
- 104.244.42.2
- 104.244.42.3
- 104.244.42.65

عنوان بروتوكول الإنترنت (104.244.42.65) يُشير إلى النطاق twitter.com، وقد وُجد أن هذا النطاق محجوب، وأظهرت القياسات التي جُمعت بواسطة برمجية أوني بروب وجود (DNS Tampering) ويُشير عنون بروتوكول الإنترنت (104.244.42.65) إلى 6 نطاقات، جميعهم كان محجوبًا:

- jhpath.com
- twitter.com
- twitter.eus
- twitter.hk
- twitter.jp
- twitter.org

أيضًا وُجد أن عنوان بروتوكول الإنترنت (104.244.42.1) محجوب (DNS Tampering) وهو عنوان يُشير إلى 5 نطاقات، جميعهم حُجبوا:

- equity-app.com
- milchreis.xyz
- twitter.com
- twittertrademarks.com
- Twopensource.com

محاولات حجب فيسبوك ماسنجر

في شهر سبتمبر 2019، أبلغ العديد من المستخدمين عن عدم قدرتهم على استخدام تطبيق فيسبوك ماسنجر على بعض شبكات الإنترنت المحمول، حيث ظهر للمستخدمين رسالة "Waiting for network" على تطبيق ماسنجر على أندرويد ورسالة "messenger is currently unavailable" على متصفحات الوِب على الحواسيب.

ويُرجّح أن تكون السلطات المصرية قد حاولت حجب موقع فيسبوك ماسنجر (messenger.com) على شبكة فودافون (ASN:AS36935) وشبكة وي (ASN:AS8452) لعدة ساعات في 23 سبتمبر 2019، قبل أن يعود للعمل مرة أخرى بشكل طبيعي.

حجب AMP

خدمة "AMP (Accelerated Mobile Pages) Project" هي تقنية تستهدف التركيز على تحسين أداء صفحات الوِب على الهواتف المحمولة، لتوفير تجربة ملائمة لمستخدمي الهواتف الذكية، حيث يوفِّر المشروع أداة مفتوحة المصدر تُمكن الناشرين على الإنترنت من زيادة سرعة تحميل وتصفح مواقعهم من خلال الهواتف الذكية،

حيث يوفِّر المشروع أداة مفتوحة المصدر تُمكن الناشرين على الإنترنت من زيادة سرعة تحميل وتصفح مواقعهم من خلال الهواتف الذكية، كما توفِّر أيضًا عرضًا بصريًا للمواقع ملائمًا للهواتف الذكية بغض النظر عن اختلاف أحجام شاشات الهواتف المحمولة والحواسيب اللوحية. ويمكن أيضًا الاستفادة من هذه المميزات لنُسَخ المواقع الموجهة للحواسيب التقليدية.

وفي فبراير ٢٠١٨، كانت العديد من المواقع الصحفية المحجوبة في مصر تستخدم خدمة صفحات الهواتف المحمولة (AMP) كمحاولة لإيجاد آليات سهلة للوصول لجمهورها كالاعتماد على منصات بديلة لنشر محتوى المواقع المحجوبة. حيث إن الاعتماد على خدمة (AMP) تُظهر روابط بديلة للروابط الأصلية في نتائج البحث على محرك بحث جوجل، بحيث تُشير إلى روابط أخرى من نطاق جوجل، ما يعني أنه في حالة أن ظهر موقع محجوب في نتائج بحث جوجل وكان هذا الموقع يستخدم صفحات الهواتف المحمولة المُسّرعة (AMP) فسيتم توجيه المستخدم لصفحة غير محجوبة وهذه هي الطريقة التي اعتمدتها بعض المواقع المحجوبة في مصر، حيث تم اعتماد الروابط المُنتجة من AMP ونشرها على الشبكات الاجتماعية لتصل إلى الجمهور دون أن يكون لديه خبرة تقنية تُمكِّنه من تجاوز الحجب. وبعد انتشار هذه الآلية لمواجهة الحجب، لجأت الحكومة المصرية إلى حجب الخدمة في ٣ فبراير ٢٠١٨، وهو ما أثر على مستخدمي الهواتف الذكية القادمين من محرك بحث جوجل لأي موقع يستخدم AMP، حيث أصبح المستخدمون غير قادرين على الوصول لهذه المواقع بما في ذلك المواقع التي لم تقم الحكومة المصرية بحجبها، ما يعني حجب مليارات الصفحات التي تستخدم تقنية (AMP) وعلى ذلك، فقد أعلنت جوجل إيقاف الخدمة في مصر.

الحجب العشوائي.. حجب المواقع القائم على حجب عنوان IP وبروتوكول TCP/IP

في إبريل ٢٠١٩، حجبت السلطات المصرية مواقع "حملة باطل" وهي حملة أطلقها نشطاء تزامنًا مع تعديلات الدستور التي دعا لها رئيس الجمهورية.

استخدمت الحملة النطاق (voiceonline.net) لموقعها الداعي إلى جمع توقيعات من مواطنين ضد التعديلات الدستورية. وفي اليوم التالي ٩ إبريل حُجب موقع الحملة بعد أن أعلنت عن جمع ٦٠ ألف توقيع رافض لتعديل الدستور. الموقع حُجب بعد ١٣ ساعة فقط من إطلاقه، ما دعا القائمين على الحملة إلى تغيير اسم النطاق لتفادي الحجب والوصول للجمهور وقد حُجبت جميع النطاقات البديلة التي أطلقتها الحملة لتصل إلى عشرة نطاقات.

في تقريرين صادرين عن مؤسسة Netblocks ومؤسسة حرية الفكر والتعبير، أظهر التقريران أن هناك آلاف المواقع التي حُجبت بسبب استخدام السلطات المصرية لتكنيك حجب المواقع القائم على حجب عنوان (IP) وبروتوكول (TCP/IP)، وذلك لأن حجب موقع واحد (حجب عنوان بروتوكول الإنترنت لموقع معين) يعني حجب أي نطاق آخر يشترك معه على نفس الخادوم ويحمل نفس عنوان بروتوكول الإنترنت.

وقد وجد التقرير الصادر عن مؤسسة حرية الفكر والتعبير أن السلطات المصرية استخدمت تكنيك حجب مواقع الوِب عن طريق حجب عنوان بروتوكول الإنترنت وحزمة بروتوكولات الإنترنت للعديد من المواقع، مثل: موقعي البورصة ودايلي نيوز إيجبت وموقع فكّر تاني وإيجبت ديلي نيوز والعربي الجديد والمرصد العربي لحرية الإعلام، بالإضافة إلى موقع حملة "باطل" وهو ما تسبب في حجب آلاف المواقع الأخرى التي تشترك معها في نفس عنوان بروتوكول الإنترنت.

حجب تليجرام

في 22 أكتوبر 2020، رصدت "مسار - مجتمع التقنية والقانون" حجب السلطات المصرية لموقع وتطبيق تلجرام، وذلك على ثلاث شبكات لمقدمي خدمة الإنترنت، وهي شبكة "وي" وشبكة "فودافون" وشبكة "أورانج" وذلك بعد إعلان العديد من مستخدمي خدمة الإنترنت على الشبكات الثلاث عدم قدرتهم على الوصول إلى "تلجرام". ويعتبر" تلجرام" واحدًا من أشهر التطبيقات المُشفّرة واسعة الانتشار في العالم.

وتأكد لمسار أن مستخدمي الشبكات الثلاث: شبكة وي (AS8452) وشبكة أورانج (AS24863) وشبكة فودافون (AS36935) لا يمكنهم استخدام تطبيق "تلجرام" على الهواتف الذكية، حيث حجبت السلطات المصرية الوصول إلى عناوين آي بي الخاصة بالتطبيق. كما حجبت السلطات موقع "تلجرام" نفسه (telegram.org) ونسخة "تلجرام" المُوجهة للحواسيب المكتبية (web.telegram.org) وشمل الحجب كذلك شبكات الإنترنت الأرضية (ADSL)، والإنترنت للهواتف المحمولة (4G/3G) أيضًا.

ساندفين في مصر

أجرت "مسار" مجموعة من الاختبارات على عينة من مواقع الوِب المحجوبة في مصر، بهدف الكشف عن استخدام مُعدات "ساندفين" لحجب هذه المواقع. وقد وجدنا 15 موقع وِب من أصل 20 موقعًا (عينة الاختبار) قد تعرّضوا للحجب بواسطة مُعدات "ساندفين". أجرت "مسار" هذه الاختبارات على خدمة الإنترنت المُقدّمة من شبكة وي (AS8452)، والتي عُرفت سابقًا بـ (تي إي داتا) والتي تُشغّلها الشركة المصرية للاتصالات، وتمتلك الحكومة المصرية 80% من أسهمها.

كان (Citizen Lab) قد نشر تقريرًا توثيقيًا حول وجود أجهزة باكيت لوجيك (PacketLogic)، وقد أشار التقرير إلى أن الحقل (IPID) يحمل بصمة "13330 (0x3412)" دائمًا، وقد طابقت هذه البصمة نفس البصمة التي وجدها الباحثون بـ"سيتزن لاب" والخاصة بأحد أجهزة باكيت لوجيك التي قاموا بشرائها.

أجهزة "ساندفين باكت لوجيك" (Sandvine PacketLogic) هي إحدى المعدات التي تُنتجها شركة "ساندفين"، وتستخدم الحكومات ومُقدِّمي خدمات الاتصالات والإنترنت أجهزة "باكت لوجيك" لإجراء عمليات الفحص العميق للحزم (Deep Packet Inspection-DPI) بحيث تُمكّنهم من مراقبة الإنترنت وحجب مواقع الوِب والتلاعب في اتصالات المستخدمين ومراقبة حركة المرور على الشبكة في الوقت الفعلي وتصفية حركة المرور على الشبكة بما في ذلك حجب مواقع الوِب وتطبيقاته وبروتوكولاته، مثل (P2P).

في مارس 2018، نشر سيتزن لاب، تقريرًا بعنوان "أزمة مرورية"، يكشف عن استخدام أجهزة "ساندفين بوكت لوجيك" في مصر، والتي استُخدمت لإعادة توجيه مستخدمي العديد من مزودي خدمة الإنترنت إلى إعلانات وسكربتات تعدين عملات رقمية. وفي 21 سبتمبر 2020، نشرت مؤسسة (Qurium) تقريرًا عن استخدام "ساندفين" لحجب موقع "المنصة"، أحد المواقع الصحفية المستقلة في مصر.

في اختبارات تحليل حزم بيانات الشبكة لعينة من المواقع المحجوبة على شبكة وي (AS8452) بواسطة برنامج (Tcpdump) وجدنا أن 15 موقع وِب من أصل 20 موقعًا (عينة الاختبار) يظهر بها نفس بصمة باكت لوجيك "13330 (0x3412)" المُشار إليها في تقرير "ساندفين".

الجدول التالي يُوضِّح ١٤ موقع وِب من أصل ٢٠ موقع ويب (عينة الاختبار) التي اكتشفنا أنها محجوبة بـ"ساندفين باكت لوجيك" :

الموقع	النطاق	التصنيف	عنوان الآي.بي
Nord VPN	nordvpn.com	أدوات إخفاء الهوية	104.17.49.74
Tor Project	torproject.org	أدوات إخفاء الهوية	95.216.163.36
الشبكة العربية لمعلومات حقوق الإنسان	anhri.net	قضايا حقوق الإنسان	213.108.104.110
المنصة	almanassa.com	وسائل إعلام	83.68.31.235
تليفزيون العربي	alaraby.tv	وسائل إعلام	152.195.32.173
حبر	7iber.com	وسائل إعلام	104.26.10.93
درب	daaarb.com	وسائل إعلام	213.108.104.107
رصيف 22	raseef22.net	وسائل إعلام	104.18.60.54
عربي 21	arabi21.com	وسائل إعلام	172.67.96.169
محيط	moheet.com	وسائل إعلام	35.231.141.67
مدى	madamasr.com	وسائل إعلام	104.26.15.160
مديم	medium.com	منصات الاستضافة والتدوين	104.16.124.127
مصر العربية	masralarabia.net	وسائل إعلام	138.201.47.90
هيومان رايتس واتش	hrw.org	قضايا حقوق الإنسان	72.251.236.179

خـاتـمـة

قامت السلطات المصرية على مدار السنوات العشر السابقة بتطوير الآليات القانونية والتقنية لحجب مواقع الوب لأسباب تتعلق بحصار المعارضة السياسية، أو منع الجمهور من الوصول إلى معلومات وآراء معينة، أو فرض رقابة على بعض المحتويات لأسباب دينية أو أخلاقية. خلال هذه الفترة طورت السلطات إستراتيجياتها القانونية من مجرد التفسير التعسفي للقوانين المنظمة للاتصالات، إلى الاعتماد على تفسيرات قضائية محافظة لمفاهيم قانونية، مثل: الأمن القومي، إلى فرض الرقابة من خلال تشريعات استثنائية مثل قانون مكافحة الإرهاب، وانتهاء بتقنين حجب المواقع بشكل نهائي في القوانين العادية سواء كجزء من إجراءات الاستدلال والتحقيق في القضايا ذات الصلة بما بات يعرف بالجرائم الإلكترونية، أو كجزاء إداري ضد مواقع الصحافة الإلكترونية من خلال المجلس الأعلى لتنظيم الإعلام.

وقد تزامن تطوير البيئة التشريعية لتقنين حجب مواقع الوِب مع تطوير تكنيكات الحجب من مجرد الاعتماد على حجب عنوان بروتوكول الإنترنت وحزمة بروتوكولات الإنترنت أو الحجب القائم على الفحص العميق للحزم، إلى استخدام معدات متطورة مثل معدات شركة "ساندفين".

ويأتي اهتمام السلطات بفرض الرقابة على الإنترنت باعتبار الفضاء السيبراني يشكل بعدًا جديدًا لما يعرف بالمجال العام، فمع نجاح السلطات في محاصرة كافة منافذ التعبير عن الرأي من الصحف، إلى الأحزاب السياسية، إلى منظمات المجتمع المدني، إلى الاحتجاج السلمي بصوره المختلفة، بقي فضاء الإنترنت عصيًا على القمع لفترة غير قصيرة، وفي نفس الوقت شكل الإنترنت مصدر قلق للسلطات بسبب الطبيعة غير المركزية لهذا الفضاء وصعوبة التحكم في المحتويات التي يتم نشرها من خلاله. حيث استطاع النشطاء جعل هذا الفضاء بديلاً لكافة المساحات الأخرى التي صادرتها السلطات لأسباب سياسية، أو دينية أو أخلاقية. وبالرغم من استمرار فاعلية الإنترنت في المجتمع المصري، فإن الجهود الرقابية التي مارستها الدولة وتحديدًا منذ عام ٢٠١٧ منعت المستخدمين من الوصول على الأقل إلى المئات من المواقع الصحفية والسياسية والثقافية، وهو ما ضاعف حجم الانتهاكات التي يتعرض لها الأفراد في السنوات الأخيرة في مجالات حرية تداول المعلومات، وحرية الرأي والتعبير وحرية الصحافة، فضلاً عن حرية استخدام الإنترنت.

https://masaar.net