# ورقة بحثية
# البيئة التقنية للمعلومات وتأثيرها على الانتخابات في ليبيا

Research Paper

The Information Technology Environment and Its Impact on Elections in Libya

2024

التعاون الألماني
DEUTSCHE ZUSAMMENARBEIT

LCFP
Libyan Center For Freedom of Press
المركز الليبي لحرية الصحافة
لإعلام مهني حر

International IDEA

المفوضية الوطنية العليا للانتخابات
High National Elections Commission

# ورقة بحثية
# البيئة التقنية للمعلومات وتأثيرها على الانتخابات في ليبيا

شوقي قدّاس

## المحتويات



ديسمبر
2024

ساهمت الثورة الرقمية في تنشيط الحياة الديمقراطية في مجتمعاتنا بإتاحة وسائل اتصال جديدة للمرشحين . وسمحت لهم هذه القنوات من التحرر من الوسطاء التقليديين وممارسة علاقة مباشرة مع الناخبين ، وهو ما جعلهم يتعرفون على الرغبات الحقيقية لناخبيهم وتركيز أنماطاً أكثر مباشرة وتشاركية للديمقراطية . كما أتاحت نفس الوسائل إلى الناخب الحصول على المعلومات بطريقة أكثر سهولة وفعالية مما كانت تقوم به وسائل الإعلام التقليدية ودون كلفة مادية ووجوب التنقل . وهو ما أنار له المشهد السياسي وأتاح له وسائل لتقييم الأوضاع والحلول المقترحة من قبل المرشحين وتبعاً لذلك اختيار أنسبهم للمناصب الانتخابية .

تطور تكنولوجيا المعلومات والاتصالات وإكسابها الطابع الديمقراطي اليوم بانتشارها في كل الأنشطة البشرية وأصقاع العالم هي فرصة حضارية ، لم تكن خياراً بل فرض على البشرية اللجوء إليها نظراً لمزاياها وحسن تقبلها من قبل الأشخاص وخاصة الشباب منهم ، ولكنها في نفس الوقت أسست لمخاطر جديدة على مجتمعاتنا . فالثورة الرقمية لم تجعل من الممكن بوسائلها المبتكرة كالذكاء الاصطناعي وضع حدّ للأزمات التي تعيشها مجتمعاتنا مثلاً في ممارسة الديمقراطية ، بل أنشأت هذه الثورة تحديات جديدة وأرست تساؤلات جديدة ولوحت بمخاطر أدت إلى وضعيات سلبية استوجبت ابتكار حلولاً جديدة لتجاوزها . فالتكنولوجيات الحديثة ككل ابتكارات البشرية تغير طريقة عيشنا وتفاعلنا مع محيطنا ومع الغير وتكون لها مزايا عديدة لا فائدة في تعدادها لبداهتها ، كما هو الحال للأدوية الحديثة فهي تسمح بشفاء المرضى وتمكينهم من نوعية أفضل من العيش لكن لمعظمها أعراضاً جانبية يجب التفطن مبكراً لها لأخذ الاحتياطات للتقليل من آثارها .
الالتجاء لتكنولوجيا المعلومات والاتصالات في إطار المسارات الانتخابية يطرح اليوم عدداً من التحديات والمخاطر التي تواجه الديمقراطيات الحديثة ، عريقة كانت أو ناشئة والتي يمكن تصنيفها إلى ثلاث فئات رئيسية :

- من ناحية ، **التهديدات المتعلقة بالأمن السيبراني** ، ولا سيما ضد المرشحين أو الناخبين أو حتى العملية الانتخابية نفسها . وتتمثل هذه المخاطر في هجومات ضارة تهدف إلى الوصول بشكل غير قانوني إلى المعطيات أو تعطيل المعالجة الرقمية لها أو إتلاف البيانات أو تزويرها أو نشرها . ويمكن أن يقوم بهذا الهجوم جواسيس ، قراصنة ، جماعات إرهابية ، دول معادية أو منظمات اجرامية دون أن ننسى الموظفين من داخل الهياكل المنظمة للعملية الانتخابية . وتكون لهذه الهجمات آثاراً سلبية على المسار الانتخابي مما يؤدي إلى فقدان ثقة الناخبين في النتائج وأيضاً في الهيئة المكلفة بتنظيم العمليات الانتخابية .

- ومن ناحية ثانية ، نشأت في السنوات الأخيرة نوع جديد من **التهديدات المتأتية من نشر الأخبار الزائفة والمضللة** التي تقوض من مصداقية العملية الانتخابية ، إذ تسمح بالتلاعب بأفكار الناخبين وتغيير تشخيصهم للواقع ، وهو ما من شأنه أن يجعلهم يتخذون قرارات مخالفة لما كانوا مقتنعين بصوابه . ولقد أثبتت التجارب المقارنة إنتشار هذه الظاهرة في كل الميادين ، ولها وقع أعمق في المسارات الانتخابية التي تتأثر بما يدور في الفضاء الرقمي ، وما يتم نشر في إطاره من معطيات فاقدة للمصداقية لا يتمعن فيها الناخب بما فيها الكفاية .

- أما من الناحية الثالثة ، يسمح تواجد المواطنين ، أي الناخبين ، بكثافة على مواقع التواصل الاجتماعي **بالتأثير الغير مشروع على خياراتهم** لا بنشر الأخبار الزائفة كما تم تقديمه سلفاً ، بل ومن خلال عملية تنميطهم ، إذ يسمح ذلك باستهداف الفئات التي يمكن التأثير عليها وذلك بجعلهم لا يطلعون إلا على أخبار مختارة موجهة لرأيهم . ويسمح هذا التلاعب بالتأثير على الخيارات الانتخابية للمواطنين والمواطنات وهو ما يؤدي إلى تغيير نتائج الانتخابات وتبعاً لذلك التشكيك في المسارات الانتخابية .

وتبعاً لما سبق بيانه ، يكون من المفيد التعرض في هذا المجال إلى التحديات والمخاطر الثلاث التي تواجه الديمقراطيات الحديثة عند لجوئها إلى تكنولوجيا المعلومات والاتصالات في إطار المسارات الانتخابية : التهديدات المتعلقة بالأمن السيبراني [1] ، ونشر الأخبار الزائفة والمضللة [2] وأخيرا بالتأثير الغير مشروع على خيارات الناخبين عبر وسائل التواصل الحديثة [4].

عند التعرض لكل من التحديات الثلاث، سيتم في مرحلة أولى وصف التهديد على حسن سير المسارات الانتخابية وفي مرحلة ثانية القيام بوصف للإطار القانوني الليبي الذي تم وضعه بغاية مجابهة هذه المخاطر والوقوف على نقائصه أو الاقرار بغيابه، وأخيراً، في مرحلة ثالثة، إقتراح حلول للحد من فاعلية تلك المخاطر على المسارات الانتخابية المقبلة في ليبيا.


1 التحول الرقمي يعمل على تعميم استخدام أدوات تكنولوجيا المعلومات والاتصالات عبر الإنترنت ويشمل في هذا الإطار الأمن السيبراني جميع الوسائل التقنية التي تضمن حماية وسلامة البيانات، سواء كانت حساسة أم لا، عبر حماية أجهزة الكمبيوتر والخوادم والأجهزة المحمولة والأنظمة الإلكترونية والشبكات والبيانات من الهجمات الضارة. ويعرف أيضا من قبل المختصين بأنه "جميع التقنيات والممارسات والسياسات التي تهدف إلى منع الهجمات السيبرانية أو التخفيف من تأثيرها. ويهدف إلى حماية أنظمة الكمبيوتر والتطبيقات والأجهزة والبيانات والأصول المالية والأفراد ضد برامج الفدية والبرامج الضارة الأخرى وعمليات التصيد الاحتيالي وسرقة البيانات والتهديدات السيبرانية الأخرى" https://www.ibm.com/fr-fr/topics/cybersecurity.

2 يقر قانون 22 ديسمبر 2018 المتعلق بالتلاعب بالمعلومات في فرنسا أنها "أي ادعاء أو إسناد لحقيقة تفتقر إلى عناصر يمكن التحقق منها من شأنها أن تجعلها محتملة" ولقد فسر المجلس الدستوري هذا المفهوم في قراره بتاريخ 20 ديسمبر بأنها "ادعاءات أو افتراضات غير دقيقة أو مضللة لحقيقة من شأنها أن تغير من صدق الانتخابات المقبلة. لا تتضمن هذه الادعاءات آراء أو محاكاة ساخرة أو أخطاء جزئية أو مبالغات بسيطة. إنها تلك التي يمكن إثبات زيفهم بشكل موضوعي. [...] لا يمكن التشكيك إلا في نشر مثل هذه الادعاءات أو الاتهامات التي تستوفي ثلاثة شروط تراكمية: يجب أن تكون مصطنعة أو آلية، وواسعة النطاق، ومتعمدة"

3 أدوات الاتصال الحديثة عبارة عن وسائط مادية أو رقمية تسمح ببث الرسائل إلى أشخاص مستهدفين محددين.

# 2 التهديدات على الأمن السيبراني وحماية المنظومة المعلوماتية الانتخابية

## 1-1 التهديدات السيبرانية خطر يترصد المسارات الانتخابية في العالم

أصبح اللجوء إلى تكنولوجيا المعلومات والاتصالات في المجال الانتخابي عملية ضرورية، ولم تعد فقط خياراً ممكناً. كل دول العالم والهياكل المكلفة بتنظيم والسهر على حسن سير العمليات الانتخابية، ولكن أيضاً المرشحين للمناصب الانتخابية والأحزاب السياسية ومنظمات المجتمع المدني، يستعينون بالقدرات الواسعة المتاحة عبر الحواسيب الضخمة والبرمجيات الذكية وشبكات التواصل السريعة لخوض أو تنظيم العمليات التي يقومون بها في إطار المسار الانتخابي. ولم يبقى الناخب خارج هذا السياق، إذ هو نفسه أصبح يعيش العملية الانتخابية عبر الوسائل الرقمية، مما جعله عرضة لعمليات إجرامية.

تقوم المسارات الانتخابية الحديثة بالتعويل المتزايد على المنظومات المعلوماتية في كل مراحلها وعملياتها. لذلك تكون الوسائل المستعملة مستهدفة بغاية المس من حسن سير العملية الانتخابية على غرار كل المنظومات المعلوماتية الأخرى.
وتتخذ عمليات القرصنة المعلوماتية في المجال الانتخابي عديد الأوجه التي تطال كل الاجهزة المستعملة والمتصلة من حواسيب، موزعات، هواتف جوالة، لوحات الكترونية أو معدات تصويت. كما تحاول هذه العمليات التدخل والاضرار بكل مراحل المسار الانتخابي، من تسجيل الناخبين وتحقق الناخبين من مكاتب الاقتراع ونشر قوائم الناخبين والمعطيات المتعلقة بالمرشحين واستعمال المعدات المخصصة للاقتراع في بعض الدول، وعملية عد الأصوات والمنصات المختلفة للتظلم أو رفع التجاوزات بطرق الكترونية والى عملية تجميع النتائج وارسالها ونشرها للعموم.

ولقد شهدت المسارات الانتخابية في العالم العديد من العمليات التي طالت المنظومات الالكترونية والتي لا يمكن سردها في إطار هذه الدراسة ونكتفي بأشهرها وأحدثها للوقوف على مخاطرها الممكنة. إذ أن المسؤولين على العمليات الانتخابية يرفضون استراتيجياً الادلاء للعموم بما آلت إليه فعلياً مثل هذه الهجومات السيبرانية لتفادي تقلص منسوب ثقة الناخبين في المنظومة الانتخابية.

يمكن تلخيص أنواع هذه العمليات من خلال الجدول المتاح في دراسة « الأمن المعلوماتي للعمليات الانتخابية » للمؤسسة الدولية للديمقراطية والانتخابات (2020) إلى الخروقات التالية التي تمس عبر تكنولوجيا المعلومات والاتصالات المستعملة في المسارات الانتخابية على ما يلي :

- هجمات الحرمان من الخدمة (DDoS).
- المسّ من مواقع الانترنت والتلاعب بمحتوياتها.
- عمليات القرصنة العامة التي تتم لأسباب إجرامية أو مالية.
- إستغلال ضعف تدابير الحماية للمنظومة المعلوماتية مثل اختراق كلمات السر الضعيفة للمستخدمين.
- عمليات تسريب للمعطيات من داخل المنظومة الالكترونية نفسها.

وتكون هذه العمليات الاجرامية متأتية من فاعل موجود على التراب الوطني أو من الخارج لكن بنفس الغاية وهي تعطيل المنظومات المعلوماتية للمس من حسن سير العمليات الانتخابية.

4 تميزت الانتخابات الرئاسية والتشريعية الأوكرانية لسنة 2014 والانتخابات الرئاسية لسنة 2019 بكم هائل من الهجمات الحاسوبية من نوع DDoS الذي يهدف إلى التغلب على موارد النظام المستهدف وجعله يتوقف عن العمل. بمناسبة الانتخابات الرئاسية لعام 2019 في مقدونيا الشمالية، جرى هجوم على أنظمة تكنولوجيا المعلومات والاتصالات التابعة للجنة الانتخابات الحكومية عبر برنامج فدية (Ransomware) الذي قيد الوصول إلى نظام الحاسوب، وطلب القراصنة بدفع فدية. كما تمكن قراصنة من الوصول إلى أنظمة اللجنة الانتخابية في المملكة المتحدة والكشف عن بيانات 40 مليون ناخب ولم يتم التفطن للهجوم الإلكتروني في أكتوبر 2022 وتبين أن أول ولوج غير شرعي للمنظومة تم في أوت 2021. رصرحت السلطات الانتخابية الروسية في 16 مارس 2024 إنه تم التصدي لحوالي 160 ألف هجوم إلكتروني ضد موارد التصويت الإلكتروني عن بعد، الذي تم تركيزه لأول مرة في روسيا. ولا يمكن التغاضي عن ذكر ما تم خلال الحملة الانتخابية لسنة 2016 في الولايات المتحدة الامريكية حيث أنه ثبت اختراق قواعد بيانات الناخبين في حوالي 40 ولاية أمريكية وشبهات لاختراق أجهزة التصويت الإلكترونية في عدة ولايات. كما يجب التعرض إلى ما تم رصده في الانتخابات الرئاسية الفرنسية لسنة 2017، إذ أطلقت الوكالة الوطنية لأمن نظم المعلومات (ANSSI) عدة تنبيهات بشأن المخاطر الرقمية التي تهدد الانتخابات، والتي أدت مثلاً إلى إلغاء إمكانية قيام الفرنسيين المقيمين في الخارج بالتصويت عبر الإنترنت خلال الانتخابات التشريعية. وفي يوم 5 مايو 2017، تمت سرقة غيغابايت من رسائل البريد الإلكتروني والوثائق من حركة «إلى الأمام» في فرنسا وتم نشرها على الانترنت وهو ما عرف بعد ذلك بفضيحة Macron Leaks.

## 2-1 تقييم للإطار القانوني والمؤسساتي الليبي

### 1. 2. 1 . تجريم الأفعال المستهدفة للمنظومات الإلكترونية

أصدرت ليبيا القانون رقم 5 بتاريخ 27 سبتمبر 2022 المتعلق بمكافحة الجرائم الإلكترونية . ولقد جاء في الفصل الثاني منه أن القانون يهدف « . . . إلى حماية التعاملات الإلكترونية ، والحد من وقوع الجرائم الإلكترونية وذلك بتحديد هذه الجرائم وإقرار العقوبات الرادعة لها ، وبما يؤدي إلى تحقيق ما يلي : . . . 5 . تعزيز الثقة العامة في صحة وسلامة المعاملات الإلكترونية» . وهو هدف كل منظومة قانونية تقرر ردع الجرائم الالكترونية ومنها اسداء كل التعاملات التي تمر بالوسائل الرقمية نفس الثقة والمصداقية التي تتسم بها التعاملات الورقية . لذلك ، وطبقاً لقواعد القانون الجزائي وخاصة مبدأ شرعية الجرائم والعقوبات ، وجب التحديد المسبق للأفعال التي يجب معاقبة مرتكبيها . وهو ما حدده الفصل المذكور من القانون عدد 5 لسنة 2022 .

كما يؤكد القانون في المادة الثالثة منه على أنه تطبق بنوده على «الجرائم المنصوص عليها فيه إذا ارتكبت كل أفعالها أو بعضها داخل ليبيا ، أو ارتكبت كل أفعالها خارج ليبيا وامتدت نتائجها وآثارها لداخل ليبيا» . ويكون بذلك ، ودون استعمال العبارات التقنية التي كرستها النصوص المقارنة ، قد قام القانون بتحديد الجرائم الالكترونية التي يقوم بها مرتكبها على التراب الوطني ولكن أيضاً من الخارج . وهي نوع من الجرائم تم تلقيبه منذ سنوات بالجرائم السيبرانية . تبعاً لذلك ، قام مكتب الأمم المتحدة الإقليمي المعني بالمخدرات والجريمة للشرق الأوسط وشمال أفريقيا على موقعه بتعريف هذا النوع من الجرائم بالتركيز على نطاقها العابر للحدود وقد وصفها : «ان الجريمة السيبرانية (اي الإلكترونية) شكل متطور من أشكال الجريمة عبر الوطنية . تزايد ضلوع جماعات الجريمة المنظمة يزيد من تفاقم الطابع المعقد لهذه جريمة ، التي تحدث في مجال الفضاء الإلكتروني الذي لا حدود له . ويمكن لمرتكبي الجرائم السيبرانية وضحاياهم أن يتواجدوا في مناطق مختلفة ، ويمكن أن تتمد آثار الجريمة عبر المجتمعات في جميع أنحاء العالم ، مما يبرز الحاجة الى وضع استجابة عاجلة وديناميكية ودولية»[5]

وتبعا لذلك السياق ، قام القانون عدد 5 لسنة 2022 بتجريم الافعال الالكترونية التي يمكن أن تهدد كل المنظومات بما في ذلك التجهيزات ، البرمجيات ، قواعد البيانات والشبكات التي تم تركيزها لمعالجة المسارات الانتخابية[6]

وبذلك ، تكون المنظومة القانونية الليبية قد وضعت القواعد التي تسمح بتجريم هذه الأفعال سواء تم ارتكابها على التراب الوطني أو من خارجه . غير أن القانون تغاضى عن بعض الأفعال الاجرامية الالكترونية التي عادة ما يتم التعرض إليها في المنظومات الالكترونية المقارنة على غرار إساءة استخدام الأجهزة ، التزوير الالكتروني والاحتيال الالكتروني .

ويكون تبعاً لما سبق بيانه ، أن الإطار القانوني الليبي قد جرّم هذه الأفعال التي يمكن أن تطال المنظومات المعلوماتية ومن بينها تلك التي تسمح بالتصرف في المسارات الانتخابية والتي يمكن أن يكون مصدرها من داخل التراب الليبي أو من الخارج للتملص من القوانين التقليدية الوطنية للقيام بأعماله الاجرامية والافلات من العقاب .

### 2. 2. 1 . إرساء منظومة تلزم على تأمين المنظومات المعلوماتية

يجب التأكيد على أن تأمين المنظومات الالكترونية يكون على صعيدين ؛ أولاً ، بإجبار المتصرفين على هذه المنظومات من اتباع قواعد وشروط تسمح بتأمينها . ثانياً ، معاقبة كل الأفعال التي تتهجم على تلك المنظومات . وإذا أوضحنا فيما سبق أن المنظومة القانونية الليبية قد أصدرت قانون يعاقب الجرائم السيبرانية ، غير أن البحث في المنظومة القانونية الليبية عبر منصة المجمع القانوني الليبي لم يسمح بالعثور على نص قانوني يتعلق بوضع القواعد الكفيلة بتأمين المنظومات الالكترونية عامة . هذا القانون تكون غايته لا تجريم الأعمال المنتهكة لسلامة المنظومات الالكترونية ، بل تحديد العمليات والأدوات والأطر التي تهدف إلى حماية الشبكات والأجهزة والبرامج والبيانات من الهجمات السيبرانية التي ترمي إلى الوصول غير المشروع إلى الأنظمة المعلوماتية ، أو تعطيل عملها العادي ، أو تغيير المعطيات أو التلاعب بها أو الاستلاء عليها ، أو القيام بالتجسس أو الابتزاز بصفة عامة ، وبالخصوص خلال المسارات الانتخابية . هذا القانون الغائب عن الإطار القانوني الوطني يسمح بالإجابة الفاعلة والاستباقية على كل العمليات الاجرامية عبر الشبكات وذلك بضمان سلامتها وتحصينها من العمليات الاجرامية .

5 https : / /www . unodc . org /romena /ar /cybercrime . html

6 التأثير في النظام الإلكتروني (المادة 10) .
الدخول غير المشروع للمنظومات (المادة 11) .
الإعتراض أو التعرض لمنظومة معلوماتية (المادة 13) .
حيازة برامج فك الترميز واستعمالها (المادة 14) .
التعدي على عمل نظام معلوماتي للحصول على منفعة مادية (المادة 15) .
التعدي على عمل نظام معلوماتي واستعمال مخرجاته (المادة 16) .
تعطيل الأعمال الحكومية (المادة 34) .
تهديد الأمن أو السلامة العامة (المادة 37) .

وعادة ما تقوم هذه المنظومات الحامية للشبكة الوطنية والمنظومات الالكترونية بإرساء هيكل وطني يكلف بالسهر على التطبيق الفعلي لقواعد السلامة المعلوماتية وإذا لزم الأمر معاقبة المسؤولين عن المنظومات الالكترونية المتقاعسين على أخذ كل التدابير التقنية والتنظيمية الكفيلة بالتقليص من مخاطر وقوع هذه الحوادث. ولقد قام القانون عدد 5 لسنة 2022 بتكليف بتلك المهام الهيئة الوطنية لأمن وسلامة المعلومات (NISSA) التي تم إنشاؤها بموجب قرار مجلس الوزراء رقم 28 لسنة 2013 [7].

ولقد نصت المادة 33 من القانون المذكور على أنه «تضع الهيئة الوطنية لأمن وسلامة المعلومات المعايير الأساسية الأمنية المعلومات وتتولى الرقابة على تحقيقها في الجهات المعنية، وعلى كل مصدر من مصادر المعلومات امتلاك وتطبيق نظم وإجراءات ووسائل أمنية معتمدة تكون كافية لحماية ما لديه من معلومات وفي كل مراحل ما يقوم به من أعمال الجمع ومعالجة وحفظ واسترجاع ونقل البيانات». وقد نص موقعها الرسمي على أنها تقوم «بتقييم ومراجعة الشبكات والأنظمة وإصدار شهادات الجودة وفقاً للمعايير الدولية وبما يتماشى مع المتطلبات المحلية، كما يقوم الفريق الفني بالهيئة بإجراء اختبارات الاختراق للتأكد من سلامة الشبكات والأنظمة والتطبيقات»، للسهر على امتثال المنظومات المعلوماتية الوطنية ومنها الانتخابية لمعايير السلامة السيبرانية.

ولقد أصدرت الهيئة «الاستراتيجية الوطنية للأمن السيبراني» التي تنص في توطئتها على «إن عملية التحول الرقمي، وبطبيعة الحال، تنطوي على عدد من التحديات والمخاطر التي يجب أن يسعى لمعالجتها، والاستعداد للتعامل مع تبعاتها والحد من آثارها السلبية. وهو الأمر الذي نسعى إلى تحقيقه عبر تبني تقنيات وآليات الأمن السيبراني. كما أنه، ومن خلال تنسيق وتوحيد جهود مؤسسات الدولة المختلفة في كل القطاعات، عبر استراتيجية وطنية للأمن السيبراني، يمكننا النجاح في تأمين وحماية هذا المجال الحيوي والحساس، وكذلك الحد من أي تهديدات أو مخاطر قد تعرقل قدراتنا على تسخير التقنية لخدمة بلادنا» [8] وقد احتوت هذه الاستراتيجية الوطنية على تسعة برامج وجب تفعيلها لضمان الأمن السيبراني للمنظومات الوطنية الرقمية، ومنها الحساسة كالمتعلقة بالتصرف في المسارات الانتخابية وهي:

- برنامج لتهيئة الأطر العامة والبيئة القانونية والتشريعية للفضاء السيبراني.
- برنامج لإنشاء وتطوير آليات متكاملة لحماية أمن الفضاء السيبراني، وتأمين البنى التحتية الحيوية للاتصالات وتقنية المعلومات.
- برنامج تجهيز البيئة الوطنية لتقنيات التشفير والتوقيع الرقمي والمصادقة على المعاملات الإلكترونية.
- برنامج بناء القدرات البشرية والخبرات الوطنية في مجال الأمن السيبراني بمختلف القطاعات.
- برنامج لدعم البحث العلمي وتعزيز روح المبادرة والابتكار وتوطين صناعة الأمن السيبراني.
- البرنامج الوطني لتعزيز ثقافة الأمن السيبراني للمجتمع لتحقيق الاستفادة الأفضل من التقنية.
- برنامج لتأهيل وضمان التزام المؤسسات الوطنية بمعايير وضوابط وسياسة الأمن السيبراني المحلية والدولية.
- برنامج لتعزيز الشراكات والتعاون الدولي والإقليمي والمحلي لتأمين الفضاء السيبراني.
- برنامج يرفع جاهزية البني التحتية لتقنية المعلومات والاتصالات، المؤسسات الوطنية لمواجهة الطوارئ والتعافي منها، وضمان استمرارية الأعمال.

وتدخل كل هذه البرامج في مجال تحسين قدرة المنظومة الإلكترونية الوطنية لمجابهة الهجومات السيبرانية والتي ستمس من حسن انجاز المسارات الانتخابية.

كما تجدر الملاحظة أن القانون أثار تخوفات مشروعة لأربعة وعشرون من بين منظمات المجتمع المدني التي أصدرت في نوفمبر 2022 بيانا تحليليا يبرز نقائص وثغرات ومخاطر تطبيق القانون [9] وطالبت فيه «مجلس النواب الليبي بإلغاء قانون الجرائم الإلكترونية فورًا». وقد ركزت المنظمات الممضية على أن القانون أستعمل «مصطلحات عامة وفضفاضة مخالفة للمعايير الدولية لحقوق الإنسان» على غرار «النظام العام» أو «الآداب العامة» وإرساء «رقابة شاملة وحجب مواقع ومحتوى دون أذون قضائية» من قبل الهيئة الوطنية لأمن وسلامة المعلومات وهو ما سيؤدي وجوبا إلى «تهديدات خطيرة لحرية الصحافة والنشر والتعبير» و«اعتداء مقنن على الخصوصية وتهديد للأمن الرقمي للمواطنين والمواطنات».

### 1. 2. 3. التعاون الدولي لمحاربة الجرائم السيبرانية

إن محاربة هذه الأعمال الاجرامية يتطلب تتبعها والقبض على مرتكبيها الذين يكونون عادة في دولة أجنبية. لذلك يستوجب إرساء إجراءات تعاون دولي تسمح بالعمل على إنفاذ القانون ومعاقبة المخالفين والمجرمين المختبئين بدول أجنبية. ولقد قام صناع القرار في أكبر عدد من دول العالم بالتكتل لمحاربة الجرائم السيبرانية التي يكون من خصائصها أنها تطال مصالح دول وأنظمتها المعلوماتية، والتي في بعض الأحيان تتسم بإستراتيجيتها كما هو الحال بالنسبة للانتخابات ويكون مصدرها متأتٍ من دولة أجنبية، وكان الحل هو الانضمام إلى معاهدة دولية تقوم بتحديد

7 https://nissa.gov.ly

8 https://nissa.gov.ly/rujubij/National__CyberSecurity__Strategy__Layout__2022__A4-1-1.pdf

9 https://menarights.org/ar/articles/mnzmat-hqwqyt-ttalb-mjls-alnwab-allyby-balgha-qanwn-aljraym-alalktrwnyt-fwraan

الإجراءات التي يجب اتباعها للقيام بالأبحاث والحصول على الاثباتات والمحافظة على الأدلة، وأخيراً تركيز هيكل تنسيقي في كل دولة عضو يقوم بربط الصلة مع نظرائه في الدول الأعضاء لضمان حسن القيام بالتتبعات ومعاقبة المخالفين.
لقد انفردت معاهدة مجلس أوروبا المفتوحة لسنة 2001 المتعلقة بالجرائم السيبرانية بوضع منظومة دولية لمحاربة هذا النوع من الجرائم. إن معاهدة بودابست تجمع اليوم 72 دولة و21 أخرى هي في طور الانضمام. كما أن محتواها كان مرجع وموضوع استلهام قرابة 80 بالمئة من دول العالم في عملية صياغة قوانينها الوطنية في هذا المجال.

## 2 المخاطر المتأتية من نشر الأخبار الزائفة والمضللة خلال المسار الانتخابي

أصبحت المجتمعات اليوم تتواصل عبر شبكات تسمح للأشخاص بالحصول على المعلومة وإيجاد مساحات نقاش حول الأوضاع التي يعيشونها والتعبير علناً عن أراءهم مع محاولة التأثير على الغير. لقد سمح تطور تكنولوجيا المعلومات والاتصالات والشبكات الاجتماعية بظهور أنماط جديدة للاتصالات، أقل مركزية وأكثر مباشرة، مما سمح بتداول المعلومات مباشرة بين الأفراد وخارج سيطرة الحكومات أو وسائل الإعلام التقليدية. وتمثل اليوم هذه الثورة في وسائل الاتصال والوصول إلى المعلومات فرصة لتنشيط ديمقراطياتنا التي سئمت الطرق القديمة في التواصل خاصة من قبل الأطراف الفاعلة من فئة الشباب. وقد سمحت هذه الوسائل بنشر أخبار زائفة ومضللة بكل سهولة، ولها آثار على حياة الأشخاص وخاصة في المجال السياسي، ويتزايد عددها ووقعها بمناسبة الانتخابات مكونة تهديداً تعاني منه كل الأنظمة السياسية (1). ولقد ركزت ليبيا هيكلاً خاصاً لتعديل المجال الإعلامي الذي يشابه مثيلاته المقارنة والتي تحاول وضع حد لهذه التجاوزات، كما تم تركيز منظومات للتعرف والتشهير بالأخبار الزائفة دون سن نص قانوني يجرم هذه الأفعال، أو على الأقل قواعد مرجعية يتم السهر على احترامها (2).

### 2-1 تهديد الأخبار الزائفة على مصداقية المسارات الانتخابية

لقد ثبت أن التطورات التكنولوجية في الاتصال أدت إلى استغلال التقنيات الحديثة للتلاعب بمواقف الناخبين وذلك عبر تطوير تداول المعلومات الكاذبة أو الزائفة. ويعزز هذا الوضع السياق العام لانعدام الثقة تجاه مصادر المعلومات التقليدية وخاصة من قبل الشباب والتي تستثمر في تطوير مصداقية المعلومات التي تقوم بنشرها. ومن المهم أن نلاحظ أن هذه التلاعبات بالمعلومات تتخذ أشكالاً شديدة التنوع، بمستويات مختلفة من التعقيد والكثافة.

إن التضليل كظاهرة اجتماعية ليس جديداً، لكن حداثته تكمن في أن التكنولوجيا الرقمية أتاحت لمختلف الجهات الفاعلة وسائل إنتاج ونشر وتضخيم المعلومات المضللة أو المتحيزة لأغراض سياسية على نطاق وسرعة غير مسبوقين، وخاصة تحديد بكل دقة هدفها. لذلك تتعرض العديد من الديمقراطيات اليوم لهجمات معلوماتية وحملات تضليل تبلغ أشدها بمناسبة المسارات الانتخابية.
إن المعلومات المضللة، التي تتواجد بشكل متزايد في وسائل التواصل الاجتماعي، وأحياناً أيضاً في وسائل الإعلام التقليدية، تشوه إمكانية إجراء نقاش عام منطقي ومعقول حول الأسئلة والقضايا التي تواجه كل مجتمع وخاصة في فترة الحملات الانتخابية. إن أعمال التقويض التي يقوم بها من يقفون وراءها نجحت في تغيير المصداقية في عدد متزايد من العمليات الانتخابية، أو حتى في زرع الشك بين الناخبين في شرعية المسارات الانتخابية، وتبعاً لذلك في المؤسسات السياسية القائمة. إن المعلومات الخاطئة تزدهر في بيئة الإنترنت.

ويكون من الصعب في هذا الإطار سرد كل الوقائع التي شهدتها مجتمعاتنا من تضليل للناخبين في إطار الحملات الانتخابية في العالم. لذلك سنكتفي بذكر أشهر حادثة في كل صنف من عمليات التضليل، أي عبر نشر الأخبار الزائفة أو التأثير على الناخبين لتوجيه خياراتهم والتي أدت إلى المس بمصداقية المسارات الانتخابية في التجارب الحديثة.

المثال الأشهر في ما يتعلق بتداول المعلومات الكاذبة أو الزائفة هو حديث العهد، ويرجع إلى طريقة انتخاب رئيس الولايات المتحدة الأمريكية دونالد ترامب سنة 2016 عندما استعمل الشائعات ومن أشهرها أن باراك أوباما ولد في كينيا، وبالتالي لا يمكن أن يصبح رئيساً. وكان المرشح لا يحب وسائل الاعلام التقليدية التي يحتقرها ويعلن عن عدم الثقة فيها وكان ينقل على تويتر أي شكل من أشكال المعلومات للوصول إلى غاياته. في سنة 2015، نشر أرقاماً كاذبة عن الجرائم التي ارتكبها الأمريكيون السود وعند مجابهته بالطبيعة الكاذبة للخبر أجاب «هل يجب أن أتحقق من كل إحصائية؟». ففي الحملة الانتخابية ضد كلينتون أكدت شركات استطلاع الرأي أن الأخبار المضللة تلقت 7.8 مليون تفاعل على الفيسبوك أما الحقيقية منها كان فقط 7.3 مليون تفاعل، وهو ما يؤكد وقع الأخبار المضللة على الناخبين.

وقد كان ترامب يهاجم وسائل الإعلام كلما سمحت له الفرصة لذلك، إذ أن دورهم كقوة مضادة والتحقق الذي تقوم به الصحافة الكلاسيكية تزعجه إلى أقصى حد، متهماً إياهم بمحاولة تشويه سمعته. وهذا الموقف أدى به إلى حد التشكيك في مؤسسات بلاده، مدعياً أن نتائج الانتخابات التي خاضها ضد جو بايدن غير حقيقية وتم التلاعب بها.

خلال الحملة الانتخابية وبغاية ربحية، إختلق كاميرون هاريس قصة مفادها أن كهربائياً عثر على بطاقات اقتراع مملوءة مسبقاً لفائدة هيلاري كلينتون في الانتخابات الرئاسية لعام 2016. وقد انتشرت هذه القصة جزئياً بسبب اتهامات المرشح ترامب آنذاك بأنه سيتم تزوير الانتخابات ضده.

كل الأخبار المضللة التي تم تداولها على وسائل التواصل الاجتماعي وبالخصوص فيسبوك وتويتر آنذاك سمحت بترجيح الكفة لصالح دونالد ترامب الذي واصل اللجوء الى الأخبار المضللة طيلة مدة رئاسته للولايات المتحدة الأمريكية. وقد لجأ إلى استعمال نفس الوسائل عند تحريض أنصاره على اقتحام مقر الكونغرس الأمريكي للاحتجاج على اعلان انتخاب بايدن مما أدى إلى فرض حظر التجوال في واشنطن وغلق حسابه على منصة تويتر.

ويمكن القيام بنفس الملاحظات في كل دول العالم التي تشهد بانتظام تطور عدد الأخبار الزائفة عند انطلاق الحملات الانتخابية. وتسمح المنصات الرقمية لمرتكبي الجريمة بالتخفي وراء هويات مستعارة يصعب كشفها على الأشخاص العادية، ولكن أيضاً على المختصين أو بالنشاط بكل حرية من خارج حدود الوطن المستهدف عبر الشبكة العنكبوتية المفتوحة والافلات من العقاب.

## 2-2 الإطار القانوني والمؤسساتي الليبي للحدّ من تأثير الأخبار الزائفة على المسارات الانتخابية

البحث في الإطار القانوني الليبي أثبت غياب قواعد يمكن أن تؤطر ظاهرة الخطاب المضلل بصفة عامة وبمناسبة الانتخابات بصفة خاصة. لكن تبين أن بعض الهياكل قد تم ارسائها لرصد هذه الظواهر المقوضة لمصداقية العملية الانتخابية ومحاولة التقليل من فاعليتها على الرأي العام.

وفي المشهد الليبي، فقد تم تركيز هيئة مختصة في هذا المجال، وهي الهيئة العامة لرصد المحتوى الإعلامي[10]، وهي الهيكل الذي تم إنشائه بقرار مجلس وزراء حكومة الوحدة الوطنية رقم 752 لسنة 2021[11]. وتختص الهيئة برصد وتتبع الاخلالات المهنية في الخطاب الإعلامي ومنها الاخبار الزائفة والمضللة في المؤسسات الإعلامية التي تستهدف ليبيا بالداخل وبالخارج. ولقد أكدت على ذلك المادة الثالثة من القرار الذي ينص على أنها تختص «... برصد وتتبع المخالفات المهنية للخطاب الإعلامي، ولها على وجه الخصوص ما يلي: متابعة خطاب الكراهية بكافة أشكاله والأخبار الزائفة والتضليل الإعلامي بوسائل الإعلام التي تستهدف ليبيا بالداخل والخارج ...». كما يرجع للهيئة «... اتخاذ كافة التدابير القانونية اللازمة ضد القنوات المرئية والمسموعة المخالفة بالتنسيق مع الجهات المحلية والدولية ذات العلاقة، سواء برفع دعاوى أو مخاطبة لجنة العقوبات بمجلس الأمن بالتنسيق مع وزارة الخارجية والتعاون الدولي ...». ويمكن للهيئة «وضع اللوائح الخاصة بالإجراءات التي تسلط على وسائل الإعلام المخالفة، من تنبيه وتحذير وإيقاف برامج إلى سحب الترخيص أو إذن المزاولة وغيره».

وتصدر قرارتها بعد اعتمادها والتصويت عليها من مجلس التقييم (الذي لم يتم بعد تركيزه) الذي يتولى النظر في الاخلالات المهنية المرتكبة. ويرأس مجلس التقييم قاض ويضم في عضويته ممثلين عن المجتمع المدني وقضاة وصحفيين وعاملين بقطاع الإعلام ممن يشهد لهم بالكفاءة والنزاهة. تضم الهيئة فريقاً مكلفاً بالرصد تم تدريبه في دورات محلية وخارجية، حيث يعمل فريق الرصد بكفاءة عالية لرصد المحتوى الإعلامي بالمؤسسات الإعلامية الليبية. ولكن الهيئة تبقى هيكل رصد وتطوير ثقافة وتدريب يقوم بدراسات وبحملات توعية وتدريبية.

وأنشأت الهيئة منصة أكدلي[12] للتحقق من الاخبار الزائفة والمضللة وترتكز على فريق متخصص معني بالتحقق من الاخبار والمعلومات المنشورة في وسائل الاعلام الليبية، وإصدار منشورات حول الزائف والمضلل منها وذلك بهدف مكافحة هذا النوع من الاخبار والمعلومات وتوعية المواطن بشأنها.

كما لا يمكن التغاضي على ذكر ما أقره القانون رقم 5 لسنة 2022 في مادته السابعة عندما نص على أنه «يجوز للهيئة الوطنية الأمن وسلامة المعلومات مراقبة ما ينشر ويعرض عبر شبكة المعلومات الدولية أو أي نظام تقني آخر، وحجب كل ما ينشر النعرات أو الأفكار التي من شأنها زعزعة أمن المجتمع واستقراره أو المساس بسلمه الاجتماعي، ولا يجوز مراقبة الرسائل الإلكترونية أو المحادثات إلا بأمر قضائي يصدر عن القاضي الجزئي المختص».

10 https://gammc.ly

11 https://lawsociety.ly/legislation/قرار-رقم-752-لسنة-2021-م-بإنشاء-الهيئة-العامة/

12 www.facebook.com/akedly.ly

كما قامت مكونات المجتمع المدني بإنشاء منصات للتحقق من الأخبار الزائفة والمضللة ومحاولة تقليص وقعها على الرأي العام ومن أهمها :

**منصة نورني**[13] للتحقق من الأخبار والمعلومات المضللة ، وهي مبادرة لصحفيين متطوعين تأسست في أبريل 2020 لمكافحة الأخبار والمعلومات المضللة ، وهي جزء من الشبكة العربية لمدققي الحقائق والشبكة الأفريقية لمدققي الحقائق . تعمل منصة نورني على التحقق من المعلومات والأخبار التي تنشر في وسائل الإعلام ووسائل التواصل الاجتماعي وتركز بشكل أساسي على المحتوى العربي المتعلق بدولة ليبيا وعلى المعلومات الصحية والخرافات والإشاعات المتعلقة بالتاريخ إضافة إلى اهتمامها وتركيزها على جوانب الأمن الرقمي ومكافحة خطاب الكراهية والتحريض .

**منصة أنير**[14] مبادرة ليبية مستقلة محايدة وغير سياسية تُعنى بشؤون الفضاء الرقمي في ليبيا ، تختص في نشر الوعي والمعرفة الرقمية ومناصرة الحقوق والسلامة الرقمية ، إضافة الى نشر ثقافة مكافحة الأخبار الزائفة .

**منصة فالصو**[15] هي منصة رقمية بحثية تعمل على مراقبة جودة المحتوي الصحفي في ليبيا ، ورصد المخالفات المهنية المتعلقة بخطاب الكراهية والتحريض ومكافحة الإشاعات والاخبار المضللة وفقاً لمنهجية بحثية قائمة على المبادئ الأخلاقية لقيم الصحافة والإعلام الحر والمسؤول ، وتهدف لتشجيع الجمهور الليبي على المساءلة الإعلامية والتبليغ عن المعلومات المضللة بهدف تحقيق التربية الإعلامية .

وقامت المنظمة الليبية للإعلام المستقل[16] بإعداد مدونة السلوك المهني الاعلامي[17] سنة 2020 ، والتي تتضمن بعض القواعد المتعلقة بالأخبار الزائفة . وعنونت النقطة الثانية «في الدقة والمصداقية» وتم التنصيص فيها بأنه : «تتحقق الدقة من خلال حصولنا على الوقائع الصحيحة ، مع توخي الصدق والابتعاد عن الاتهامات والتكهنات غير المستندة إلى دليل . وتتطلب منا معالجة المعلومات والبحث عن الأدلة وتمحيصها ، وتنويع الآراء ، والتثبت من المعلومات أو الأخبار .

ولتحقيق ذلك ، يتطلب منا أن :

- نتبع الوسائل والطرق المشروعة للحصول على المعلومات ، فلا نوظف المال وما يفيد حكمه مقابل معلومات مضللة أو مفبركة .
- تكون كل المواد الإعلامية المقدمة للجمهور مسنودة إلى مصادر واضحة ، ومبينة على أدلة سليمة .
- نتأكد من أصلية ومصادر أية وثائق مكتوبة أو مصورة تتضمن معلومات تستحق النشر ، كما يجب علينا التثبت من أي أرقام أو إحصائيات وذكر مصادرها .
- نتجنب نشر أية أخبار دون التثبت من صحتها بصورة قاطعة ، وإذا دعت الضرورة الملحة إلى بث أو نشر خبر غير مؤكد ، ولم يكن يمكن التحقق منه بما فيه الكفاية ، ينبغي الإشارة إلى ذلك ونقول "ولم يتسند ، تأكد من مصادر أخرى" .

كما يمكن توخي الحل الذي تم ابتكاره في الفضاء الأوروبي والمماثل لما تم القيام به من قبل المنظمة الليبية للإعلام المستقل ، أي إصدار قواعد مرجعية لحث وسائل الاعلام على توخي الاحتياطات اللازمة لتجنب نشر وتوزيع الاخبار المضللة . وهو ما كان موضوع ما تم إقراره في 2022 من[18] «قواعد الممارسات المعززة بشأن المعلومات المضللة» . وكانت الغاية من هذه المدونة التي تجمع قواعد الممارسة الأخلاقية على تمكين الاعلام من الالتزام بمعايير التنظيم الذاتي لمكافحة المعلومات المضللة ووضع التزامات وتدابير طموحة تهدف إلى مكافحة المعلومات المضللة عبر الإنترنت . كما تجمع المدونة الجديدة بين مجموعة أكثر تنوعاً من أصحاب المصلحة أكثر من أي وقت مضى ، وتمكنهم من المساهمة في تحسينات واسعة النطاق من خلال التوقيع على التزامات محددة ذات صلة بمجال عملهم . وتشمل هذه الالتزامات منع نشر المعلومات المضللة ؛ ضمان شفافية الإعلانات السياسية ؛ تعزيز التعاون مع مدققي الحقائق ؛ وتسهيل وصول الباحثين إلى البيانات . «إن دعم المنصات والصناعة للوفاء بالتزاماتها بموجب مدونة ممارسات التضليل يغذي التزام المفوضية الأوروبية ببيئة أكثر شفافية وأماناً وجديرة بالثقة على الإنترنت» .

13 https://nawerny.org.ly
14 https://annir.ly
15 https://falso.ly
16 lofim.org.ly
17 https://lofim.org.ly/download/مدونة-السلوك-المهني-الاعلامي/#
18 https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

# 3 تهديدات التأثير على خيارات الناخبين عبر وسائل التواصل الاجتماعي

وضعية أخرى للتدخل الغير شرعي في المسارات الانتخابية هي أكثر غدراً، والتي تلجأ إلى تقنيات تستهدف الناخبين للتعرف بشكل أفضل ودقيق على كل واحد منهم على حدة **لتنميطهم وتبعاً لذلك تكييف المعلومات التي يتلقونها** وفقاً لمصالح والتوجهات السياسية للفاعل.

## 3-1 مخاطر التلاعب بالناخبين عبر وسائل التواصل الاجتماعي

وضعية مماثلة للتي سبقتها تتعلق بالتأثير على الخيار السيادي للناخبين بمحاولة تنميطهم (بتقسيمهم الى فئات) من خلال منصات التواصل وتوجيه أنظارهم نحو أخبار معينة تجعلهم يقتنعون بصواب ما يدعون اليه وتغيير خياراتهم السياسية بمناسبة الانتخابات. على منصات التواصل الاجتماعي خاصة، وفي خرق واضح لخصوصية الأشخاص وحماية معطياتهم الشخصية، يتم تنميط الناخبين لتحديد المجموعات القابلة للتأثير والعمل عبر توجيه الخوارزميات على مدهم بالمنشورات والمعلومات التي ستسمح بتغيير مواقفهم وخياراتهم السياسية.

التأثير على الناخبين بهذه الطريقة الغير شرعية وقانونية تم معاينتها في مناسبات عديدة في عدد من الديمقراطيات، كما تمت في بعضها معاقبة من ساهم في مثل هذا التلاعب بالناخبين وخياراتهم السيادية. المثال الأكثر شهرة في هذا المجال يبقى فضيحة كامبريدج أناليتيكا Cambridge Analytica في إستفتاء Brexit في 2016 الذي أدى إلى خروج بريطانيا من الاتحاد الأوروبي ونفس السنة انتخاب دونالد ترامب لرئاسة الولايات المتحدة الأمريكية والذي أدى إلى معاقبة فيسبوك في 2018 لسماحه بالتأثير الغير قانوني على الناخبين.

وأحسن مثال كان له الأثر الكبير، هو ما حصل في فضيحة كامبريدج أناليتيكا وهي شركة بريطانية مختصة في البرمجيات ومعالجة المعطيات، والتي تحصلت على قاعدة بيانات عدد كبير من مشتركي منصة فايسبوك بتواطؤ منها. وكانت الغاية من ذلك أن يتم عن طريق برمجية تسمح بتجميع هذه البيانات الشخصية مع بيانات أخرى ذات أهمية انتخابية، حتى تتمكن بعد ذلك من التلاعب النفسي بالناخبين من خلال الرسائل التي تستهدفهم على وجه التحديد، بناءً على ملفهم النفسي على الشبكات الاجتماعية. وقد كشف العديد من المبلغين عن المخالفات التي تم ارتكابها من قبل كامبريدج أناليتيكا لفائدة أحزاب مؤيدة لخروج بريطانيا من الاتحاد الأوروبي.

وقد تم إثبات بعد ذلك أن هذا التأثير الغير شرعي عل الناخبين عبر منصات التواصل تم اللجوء إليه في انتخاب ترامب في الولايات المتحدة الأمريكية ورئيس البرازيل بعد ذلك، وهو ما أدى بعد حل شركة كامبريدج أناليتيكا بالتغريم التاريخي لفيسبوك من قبل وكالة حماية المستهلك الأمريكية (FTC) بغرامة تبلغ 5 مليارات دولار في صيف عام 2019 التي تم إقرارها من قبل القضاء في أبريل 2020.

وتبرز هذه الطريقة في تقويض المسار الانتخابي بالتأثير على الناخبين بتوجيه اهتمامهم وإقناعهم بصحة الخيار عبر تقليص اتاحة الأخبار والمنشورات الى تلك المؤيدة فقط لذلك التوجه. في كل الحالات يتم التلاعب بالخيار المستقل والسيادي للناخب وتقويض حسن سير المسار الانتخابي. ولا يمكن القيام بهذا التلاعب بالناخبين إلا إذا تم ذلك في دولة لا تحمي المعطيات الشخصية للأشخاص على ترابها، كما هو الحال في قرابة 160 دولة في العالم. ويكون هذا التلاعب ممكناً في دول غير حامية للمعطيات الشخصية كالولايات المتحدة الامريكية.

## 3-2 الإطار القانوني الليبي ونقائصه في مجابهة هذه المخاطر

للانتخابات إطار قانوني يحدد القواعد التي يجب إحترامها طيلة المسار من قبل الأطراف القائمة عليها. ويقوم عادة بتحديد الخروقات الممكن ارتكابها والعقوبات التي تنتج عنها لغاية منعها أو على الأقل التقليص منها. لكن اللجوء إلى التقنيات الحديثة أثار إشكاليات جديدة تثير مصاعب لصناع القرار والمشرع لوضع قواعد قانونية نافذة تحد من هذه المخالفات أو الأعمال الاجرامية. وتبرز الصعوبة الأولى على مستوى تعريف الأفعال والمفاهيم الحديثة على غرار الذكاء الاصطناعي أو في مجال دراستنا كالتنميط مثلاً، والتي لم يعرفها أي نص قانوني في المنظومات القانونية الليبية. ويكون تبرير الفجوة بين الواقع والنص القانوني الذي مطالب بتأطيره يرجع إلى سرعة تطور المجالات التكنولوجية وبطء بلورة القرارات السياسية والقانونية. وهو ما ألزم المجتمعات المتطورة على تركيز هياكل تعديلية ورقابية تقنية تتمتع بالاستقلالية على السلطة السياسية وخاصة بالسلطة الترتيبية التي تسمح لها بإصدار القواعد الالزامية المؤطرة لمجال معين.

لقد أثبتت الحلول المقارنة أنه يمكن مجابهة هذه الظاهرة وعلى الأقل التقليص من وقعها بضمان حماية الحياة الخاصة للناخبين من جهة وإمكانية التحقيق ومعاقبة المنصات المسؤولة على تلك الأفعال من جهة أخرى. لقد أقرت قرابة 150 دولة في العالم قوانيناً حامية للمعطيات الشخصية تلزم صاحب المنصة على احترام مبدأ النزاهة والشفافية والذات البشرية عند معالجة معطيات الأشخاص، ويعاقب كل خرق لقواعد الحماية. وليبيا لم تسن بعد قانوناً حام للمعطيات الشخصية.

كما أوجب القانون الفرنسي رقم 1202-2020 مثلا على منصات التواصل الاجتماعي تعيين ممثل قانوني دائم على التراب الوطني يعمل كجهة اتصال مع السلطات العمومية والقضاء، وهو نفس التوجه الذي تم إقراره في الأردن.

## 4 مقترحات تطوير مصداقية منظومات تكنولوجيا المعلومات والاتصالات في إطار المسارات الانتخابية

تبعاً لما تم بيانه ولغرض تحصين المسارات الانتخابية ضد إمكانية المس من أمن منظوماتها المعلوماتية، يكون من المستحسن النظر في إمكانية الالتجاء إلى الحلول التالية:

- من الضروري والمتأكد **تعديل القانون عدد 5 لسنة 2022** لإدراج بعض الجرائم التي تغافل عنها المشرع في النسخة الحالية.
- من المقترح **إصدار قانون وطني متعلق بالسلامة المعلوماتية**، الذي سيضع قواعد تأمين المنظومات الالكترونية والذي سيسند للهيئة الوطنية سلطة ونفوذاً أوسع للسهر على حسن تطبيق قواعد السلامة المعلوماتية من قبل المتصرفين في المنظومات ومنها الانتخابية. ويجب أن تتسم الهيئة بالاستقلالية وتتمتع باختصاص تقني يسمح له بتعديل التدخلات في مجال تأمين الفضاء السيبراني وإصدار القواعد المرجعية التي يتجه إلى كل هيكل عام أو خاص إحترامها في الفضاء السيبراني.
- من المستحسن أن يتم **الانضمام لمعاهدة بودابست لمجلس أوروبا** التي تسمح بتركيز منظومة تعاون دولي لتتبع ومعاقبة الأفعال الاجرامية المستهدفة للمسار الانتخابي الليبي مهما كان مصدرها، وهو ما سيسمح بتفعيل إجراءات التقصي والحصول على الاثباتات لمعاقبة المجرمين أينما كان مكان القيام بهذه الأعمال الاجرامية نظراً لكون الجريمة السيبرانية هي عابرة للحدود.

ومن جهة أخرى فإن محاربة ظاهرة الأخبار الزائفة والمضللة وعمليات التأثير الغير مشروع على الناخبين من خلال الاستعمال الغير أخلاقي لتكنولوجيات المعلومات يمر باتخاذ التدابير التالية للحد من تأثير الأخبار الزائفة والخطاب المظلل على المسارات الانتخابية:

- اصدار **تشريع يسمح بحجب الخطاب المضلل** وخاصة في غضون المسارات الانتخابية وعلى منصات التواصل الحديثة دون أن تكون وسيلة تحد من حرية التعبير والصحافة.
- **إسناد الهيئة العامة لرصد المحتوى الإعلامي أكبر نفوذاً ووسائل** رصد للتجاوزات وتعديل المجال الإعلامي بغاية تركيز ثقافة مسؤولة وتوعية المتلقين للأخبار والقيام بأخذ التدابير السريعة لمعاقبة المتجاوزين ووضع حد لهذه الظاهرة.
- إتخاذ تدابير قانونية وعملية تجعل من عملية نشر المعلومات على المنصات أكثر شفافية حول من **يقوم بذلك وبأي تمويلات** خاصة خلال الحملة الانتخابية.
- وضع **معايير مرجعية لوسائل الاعلام والتواصل الرقمي** وإسناد شارة خاصة للمنصات التي تعمل على منع بث الخطاب المُضلل والتحقق من صحة المعلومات قبل بثها.

وأخير في ما يتعلق بتأثير على الناخبين عبر وسائل التواصل الحديثة يقترح الالتجاء إلى الحلول المتعلقة بالحد من هذه ظاهرة الشائعة اليوم في التجارب المقارنة والمتمثلة خاصة في:

- تأطير وسائل التواصل الاجتماعي الأجنبية **وإلزامهم بتركيز تمثيل لهم على التراب الوطني** لإلزامهم باحترام القوانين الوطنية ومعالجة معطيات الأشخاص طبقاً لقواعد حمايتها.
- التسريع في إصدار **قانون متعلق بحماية البيانات الشخصية** على التراب الوطني، والذي يسمح بحماية الحياة الخاصة للأشخاص الطبيعيين ووضع شروط لمعالجة معطياتهم والتواصل معهم وخاصة بغاية تنميطهم للتأثير عليهم. وهو ما تنكب عليه حاليا لجنة صياغة تقدمت أعمالها.





# البيئة التقنية للمعلومات وتأثيرها على الانتخابات في ليبيا

Research Paper

# The Information Technology Environment and Its Impact on Elections in Libya

ديسمبر
2024