



نتائج مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية

قيادة مبادرة أنير بالتعاون مع مجتمع الإنترنت - ليبيا.

أكتوبر 2024



ملخص تنفيذي عام

في عصر التقدم الرقمي السريع، تقف ليبيا عند عتبة استخدام التكنولوجيا لدفع التنمية الاقتصادية، وتعزيز الخدمات العامة، ورفع مستوى حياة مواطنيها. ومع ذلك، تتطلب هذه التحولات الرقمية نهجاً استراتيجياً وشاملاً للتعامل مع التحديات والفرص المتاحة.

تقدم مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية، بالتعاون مع مجتمع الإنترنت - ليبيا، سلسلة من الملخصات السياسية المصممة لوضع خطة وتنفيذ إجراءات استراتيجية لمستقبل ليبيا الرقمي. وقد تم تطوير هذه الملخصات بالاعتماد على إطار عمل ROAR الخاص بمنظمة اليونسكو (Robustness - الحقوق، الانفتاح، إمكانية الوصول، والمتانة)، مما يضمن منهجية شفافة وقائمة على الأدلة. شارك في تطوير هذه الملخصات السياسية مجموعة واسعة من أصحاب المصلحة، بما في ذلك:

- الأكاديميون
- ممثلو القطاع الخاص
- منظمات المجتمع المدني (NGOs)
- المحامون والخبراء القانونيون
- خبراء التكنولوجيا المستقلون
- عدة مؤسسات حكومية

تعالج هذه الملخصات السياسية جوانب حرجية مثل أمن المعلومات الرقمية، حقوق الإنترنت، الخصوصية، والشمولية الرقمية. الهدف هو تنمية بيئة رقمية تولي أهمية للأمان، الشمولية، واحترام حقوق الإنسان، مع تبني أفضل الممارسات الدولية وضمان ملاءمتها للسياق الليبي.



جدول المحتويات

2	موجز سياسة حول الأمن السيبراني في ليبيا
2	الملخص التنفيذي
2	التوصيات الرئيسية
2	المقدمة
2	الأهداف والغايات الاستراتيجية
3	التحديات الرئيسية
3	المبادرات والسياسات والقرارات والقوانين الرئيسية المتعلقة بالأمن السيبراني في ليبيا حتى عام 2024
5	أبرز المبادرات المنفذة
5	التوصيات والسياسات والإجراءات المقترحة
6	الإطار التنفيذي (ROAR)
6	المراقبة والتقييم
6	الخاتمة
7	موجز سياسة حول الحيز الرقمي من منظور حقوق الإنسان في ليبيا
7	الملخص التنفيذي
7	التوصيات الرئيسية
8	المقدمة
8	الأهداف والغايات الاستراتيجية
8	التحديات الرئيسية
8	التوصيات والإجراءات السياسية
9	المبادرات والسياسات والقوانين الرئيسية المتعلقة بالرقمنة من منظور حقوق الإنسان في ليبيا حتى عام 2024
9	الإطار التنفيذي (ROAR)
10	الرصد والتقييم
10	الخاتمة
11	موجز سياسة حول حماية خصوصية البيانات الشخصية في ليبيا
11	الملخص التنفيذي
11	التوصيات الرئيسية
11	مقدمة
11	السياق الحالي
12	الأهداف والغايات الاستراتيجية
12	التحديات الرئيسية
12	التوصيات لتأسيس سياسة وطنية للخصوصية
13	مواءمة سياسة الخصوصية الوطنية مع مبادئ ROAM الخاصة باليونسكو
13	الرصد والتقييم
14	الخاتمة
1	الملاحظات الختامية
1	المنهجية
1	البيانات
1	الملحق 1: الموارد والأدوات الداعمة
1	حقوق النشر والمعلومات



موجز سياسة حول الأمن السيبراني في ليبيا

الملخص التنفيذي

في عصر التحول الرقمي السريع، تواجه ليبيا تحديات متصاعدة في مجال الأمن السيبراني تهدد البنية التحتية الحيوية والبيانات الحساسة والأمن الوطني. إن الاعتماد المتزايد على التكنولوجيا يتطلب بيئة رقمية آمنة لدعم العمليات الحكومية والأنشطة الاقتصادية والتنمية الاجتماعية. ومع ذلك، فإن الزيادة الأخيرة في الهجمات السيبرانية – وخاصة تلك التي تستهدف القطاعات الحكومية والمالية – تؤكد الحاجة الملحة إلى استراتيجية قوية للأمن السيبراني لمعالجة نقاط الضعف الحالية والمخاطر المستقبلية.

التوصيات الرئيسية

1. إنشاء هيئة وطنية للأمن السيبراني
2. تطوير إطار قانوني شامل
3. إطلاق برامج توعية وتدريب وطنية
4. الاستثمار في البنية التحتية والتقنيات الحديثة
5. تعزيز التعاون الدولي

المقدمة

ليبيا، كغيرها من الدول في العصر الرقمي، تواجه تحديات متزايدة في مجال الأمن السيبراني مع الاعتماد المتنامي على التكنولوجيا والإنترنت. في عام 2023، لوحظ ارتفاع ملحوظ في الهجمات السيبرانية والجرائم الإلكترونية التي استهدفت بشكل خاص القطاعات الحكومية والمالية، بالإضافة إلى التعرض للبيانات الشخصية للمواطنين. وقد أفادت عدة مصادر محلية بوقوع هذه الهجمات، إلا أن غياب توثيق رسمي أو تقارير موثوقة يجعل من الصعب تقييم حجم وتأثير هذه التهديدات بدقة. مقارنة بالدول المجاورة، تعاني ليبيا من تأخر نسبي في تطوير استراتيجيات وطنية للأمن السيبراني، حيث أطلقت تونس استراتيجيتها الوطنية في عام 2019، بينما في ليبيا في ليبيا في أطلقت الهيئة الوطنية لأمن وسلامة المعلومات في فبراير 2023 الإستراتيجية الوطنية للأمن السيبراني كإطار عام لحماية البيانات وتعزيز الدفاعات الإلكترونية.

تُعد الإستراتيجية الوطنية للأمن السيبراني في ليبيا (2023)¹ أساسًا قويًا لتعزيز الصمود السيبراني، لكن فعاليتها تعتمد على آليات تنفيذ واضحة، وهياكل مساءلة، والتعاون الدولي. ويتطلب نجاحها تعزيز خطط التنفيذ، وتحسين الحوكمة، وضمان التمويل المستدام.

الأهداف والغايات الاستراتيجية

تهدف سياسة الأمن السيبراني إلى إنشاء بنية تحتية رقمية مرنة وآمنة في ليبيا. تشمل الأهداف الرئيسية ما يلي:

1. تطوير بنية تحتية رقمية قوية: بناء أنظمة وشبكات قادرة على تحمل الهجمات السيبرانية.
2. حماية البيانات الحساسة: تأمين المعلومات الحيوية لحماية المصالح الوطنية.
3. تعزيز القدرات المؤسسية: تحسين مهارات وخبرات المؤسسات الوطنية في مجال الأمن السيبراني.

¹ الهيئة الوطنية لأمن وسلامة المعلومات أطلقت في فبراير 2023 [الاستراتيجية الوطنية للأمن السيبراني](#)، التي تعتبر الإطار العام الذي يساعد المؤسسات الحكومية على وضع استراتيجياتها الخاصة لحماية بياناتها.



4. دعم التحول الرقمي الآمن: تسهيل الانتقال الآمن والسلس إلى الأنظمة الرقمية عبر جميع القطاعات.

التحديات الرئيسية

- على مدار 12 شهرًا من الاجتماعات المكثفة، والطاولات المستديرة، والنقاشات المستفيضة، عملت مجموعة العمل على تحديد أبرز التحديات التي تعيق تطوير وتعزيز الأمن السيبراني في ليبيا، والتي تشمل:
1. ضعف البنية التحتية: شبكات اتصالات قديمة ومراكز بيانات غير آمنة، واتساع الرقعة الجغرافية يزيد من صعوبة تأمين الشبكات.
 2. نقص الكوادر المتخصصة: نقص حاد في المتخصصين المعتمدين في الأمن السيبراني، وغياب برامج تعليمية متخصصة في الجامعات الليبية.
 3. التقلبات السياسية والاقتصادية: عدم الاستقرار السياسي وتعدد الجهات المسؤولة يعيق تنفيذ سياسات طويلة الأمد، ومحدودية الموارد المالية وصعوبة جذب الاستثمارات الأجنبية في قطاع تكنولوجيا المعلومات.
 4. التهديدات الخارجية والمخاطر الرقمية: ارتفاع الهجمات السيبرانية الموجهة من جهات خارجية، مخاطر في عملية التحول الرقمي وانتشار إنترنت الأشياء (IoT).
 5. التطور التكنولوجي السريع: ظهور تقنيات الجيل الخامس (5G) وتحدياتها الأمنية، وتهديدات الذكاء الاصطناعي والحوسبة الكمومية لأنظمة التشفير الحالية.
 6. الموازنة بين الأمن والخصوصية: تحدي حماية البيانات الشخصية مع ضمان الأمن القومي، والحاجة إلى أطر قانونية وتقنية متوازنة.
 7. نشر الوعي السيبراني: تحدي نشر ثقافة الأمن السيبراني بين مختلف شرائح المجتمع، والحاجة إلى برامج تعليمية مستمرة ومتطورة.

المبادرات والسياسات والقرارات والقوانين الرئيسية المتعلقة بالأمن السيبراني في ليبيا حتى عام 2024

1. قرار وزير الاقتصاد رقم (150) لسنة 2024 بشأن تنظيم نشاط مزاوله خدمات الأمن السيبراني المعدل بالقرار رقم 213 لسنة 2024
 - يفرض الترخيص الإلزامي لمزودي خدمات الأمن السيبراني تحت إشراف جهاز المخابرات العامة.
 - يعزز الإطار التنظيمي للأمن السيبراني ويدمج متطلبات الترخيص في عملية الحصول على تراخيص الأعمال.
2. قانون رقم (05) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية.
 - يهدف إلى مكافحة الجرائم الإلكترونية من خلال وضع إطار قانوني لتجريم الأنشطة غير المشروعة في الفضاء السيبراني.
 - يشمل الأحكام المتعلقة بمكافحة الاحتيال الإلكتروني، واختراق الأنظمة، وسرقة الهوية الرقمية.
 - يمنح السلطات المختصة صلاحيات لإنفاذ القانون، مثل حجب المواقع الضارة، وتتبع الجناة، وفرض العقوبات على المخالفين.
 - يتضمن عقوبات مشددة تصل إلى الغرامات المالية والسجن بحق مرتكبي الجرائم السيبرانية التي تهدد الأمن الوطني والاقتصادي.
3. قانون رقم (06) لسنة 2022 بشأن المعاملات الإلكترونية.



- ينظم استخدام الوسائل الإلكترونية في التبادلات التجارية والخدمات الحكومية لضمان أمن وموثوقية المعاملات الرقمية.
 - يعترف بالتوقيع الإلكتروني، والعقود الإلكترونية، والسجلات الرقمية كوثائق قانونية معترف بها.
 - يشمل إجراءات لحماية خصوصية البيانات وضمان سرية المعلومات الشخصية والمالية أثناء المعاملات الرقمية.
 - يحدد المسؤوليات القانونية لمزودي الخدمات الرقمية ويلزمهم بالامتثال لمعايير الأمن السيبراني
4. الاستراتيجية الوطنية للأمن السيبراني المنبثقة عن الهيئة الوطنية لأمن وسلامة المعلومات في 2023
- تهدف إلى تحديد نهج ليبيا في تأمين البنية التحتية السيبرانية وحماية البيانات الحيوية والتصدي للتهديدات السيبرانية.
 - تشمل الأهداف الرئيسية تعزيز قدرة البنية التحتية الوطنية، حماية بيانات المواطنين، وتوفير بيئة رقمية آمنة لتحقيق النمو الاقتصادي.
5. الهيئة الوطنية لأمن وسلامة المعلومات
- تأسست بموجب القرار رقم (28) لسنة 2013 الصادر عن مجلس الوزراء، كجهة مختصة بتنسيق وتنفيذ سياسات الأمن السيبراني في ليبيا.
 - تتولى الإشراف على تنفيذ التدابير الأمنية السيبرانية في جميع أنحاء البلاد.
 - تلعب دوراً حاسماً في ضمان الالتزام بالسياسات الوطنية والمعايير الدولية في مجال أمن المعلومات.
 - تقوم بتنظيم ممارسات الأمن السيبراني، ومراقبة الالتزام بالقوانين واللوائح، ودعم تطوير القدرات السيبرانية.
 - تشمل مهامها تطوير السياسات والمعايير الوطنية، توفير خدمات المصادقة والتشفير، والإشراف على حوكمة الإنترنت والاستجابة للحوادث السيبرانية.
6. قوانين حماية البيانات
- تعمل ليبيا على تقديم لوائح لحماية البيانات الشخصية وضمان خصوصية المواطنين في الفضاء الرقمي.
 - تعتبر هذه القوانين جزءاً لا يتجزأ من إطار الأمن السيبراني الأوسع.
7. مبادرات حماية البنية التحتية الحيوية
- تُركز مبادرات حماية البنية التحتية الحيوية في ليبيا على تأمين القطاعات الأساسية مثل الاتصالات، الطاقة، والخدمات المالية من التهديدات السيبرانية.
 - تتضمن هذه المبادرات تنفيذ تدابير أمنية سيبرانية متقدمة، وبروتوكولات للاستجابة للحوادث، وشراكات بين القطاعين العام والخاص لضمان استمرارية الخدمات الحيوية وتعزيز القدرة على التصدي للهجمات السيبرانية.
8. التعاون والاتفاقيات الدولية
- شاركت ليبيا في صياغة اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية، والتي تهدف إلى تعزيز الأمن السيبراني ومنع الجرائم الرقمية.
 - الاتفاقية العربية لمكافحة جرائم تقنية المعلومات: تهدف إلى تعزيز التعاون العربي في مكافحة الجرائم الإلكترونية وحماية الأمن الرقمي للدول الأعضاء.
 - تعمل الهيئة الوطنية لأمن وسلامة المعلومات على تطوير شراكات دولية وإقليمية لتعزيز قدرات ليبيا في حماية البنية التحتية الرقمية ومكافحة التهديدات السيبرانية.



- ادعت ليبيا اتفاقية أممية ملزمة قانونيًا لمكافحة الجريمة السيبرانية، مما يعكس جهودها في التنسيق مع المجتمع الدولي.

أبرز المبادرات المنفذة

1. تعزيز الأمن السيبراني وحماية البنية التحتية الرقمية: تعمل الهيئة الوطنية لأمن وسلامة المعلومات بالتعاون مع المؤسسات الحكومية والقطاع الخاص لضمان حماية البنية التحتية الرقمية من الهجمات السيبرانية المتزايدة التي تستهدف ليبيا.
2. استراتيجية التحول الرقمي²: أطلقت حكومة الوحدة الوطنية استراتيجية للتحول الرقمي تهدف إلى تطوير البنية التحتية الرقمية الأساسية، وتسهيل الوصول إلى الخدمات الحكومية، وضمان أمن المعلومات.
3. إعادة تأهيل البنية التحتية المتضررة: في عام 2016، أطلقت وزارة التخطيط بحكومة الوفاق الليبية بالتعاون مع برنامج الأمم المتحدة الإنمائي مشروعًا لإعادة بناء البنية التحتية المتضررة، بهدف تحسين الخدمات الأساسية في المناطق المتضررة من النزاعات.

التوصيات والسياسات والإجراءات المقترحة

تم إعداد هذه التوصيات من قبل مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية، والتي تضم طيفًا واسعًا من أصحاب المصلحة، بما في ذلك الأكاديميين، ممثلي القطاع الخاص، منظمات المجتمع المدني (NGOs)، المحامين والخبراء القانونيين، خبراء التكنولوجيا المستقلين، وعدة مؤسسات حكومية. وتتمثل هذه التوصيات في:

1. الإطار القانوني:
 - صياغة تشريعات شاملة للأمن السيبراني تتماشى مع المعايير الدولية.
 - دمج متطلبات الأمن السيبراني في لوائح تراخيص الأعمال.
2. التطوير المؤسسي:
 - تشكيل هيئة وطنية للأمن السيبراني للإشراف على جهود الأمن السيبراني وتنسيقها.
3. التوعية والتعليم:
 - إطلاق حملات وطنية لتوعية الأفراد والمؤسسات بأفضل ممارسات الأمن السيبراني.
4. الإجراءات الفنية والاستثمار في البنية التحتية:
 - تحديث شبكات الاتصالات ومراكز البيانات وغيرها من البنى التحتية الرقمية الحيوية.
5. التعاون الدولي:
 - تعزيز الشراكات الدولية لتبادل المعرفة وتحسين القدرات السيبرانية.

² الاستراتيجية الوطنية للتحول الرقمي 2023 - 2030: تعرض هذه الوثيقة الاستراتيجية الوطنية للتحول الرقمي الحكومي، والتي تعمل على تأطير كل الجهود والمبادرات التي تمت في السابق وتحدد المسارات الواجب اتباعها للدفع باتجاه بناء دولة عصرية بحكومة ذكية ومفتوحة وشفافة ومسؤولة.



الإطار التنفيذي³ (ROAR)

يستند الإطار التنفيذي (ROAR) إلى أفضل الممارسات العالمية في مجال الأمن السيبراني، وهو مستوحى من إرشادات المنظمات الدولية مثل المعهد الوطني للمعايير والتقنية (NIST) والاتحاد الدولي للاتصالات (ITU) ومنهجيات الأمن السيبراني الحديثة. تم تطوير هذا الإطار لمساعدة الدول والمؤسسات على تحسين قدراتها الدفاعية ضد التهديدات السيبرانية وتعزيز استجابة فعالة للحوادث الإلكترونية.

باعتبار ليبيا تواجه تحديات متزايدة في الأمن السيبراني ونقص البنية التحتية الرقمية المتطورة، يوفر إطار ROAR فرصة لتطوير منظومة وطنية للأمن السيبراني قادرة على التصدي للهجمات الرقمية وحماية القطاعات الحيوية مثل الاتصالات، الطاقة، والخدمات المالية.

ويعتمد الإطار على أربعة ركائز أساسية:

- المرونة (Resilience): تطوير خطط طوارئ واستمرارية الأعمال للتعامل مع الحوادث السيبرانية، مع إجراء تقييمات دورية للمخاطر ونقاط الضعف في الأنظمة الرقمية.
- المراقبة (Observability): إنشاء مراكز عمليات أمنية (SOC) لرصد وتحليل الأنشطة السيبرانية بشكل مستمر، واستخدام أدوات وتقنيات متقدمة للكشف المبكر عن التهديدات.
- الأتمتة (Automation): تطبيق حلول أتمتة لتعزيز كفاءة وسرعة الاستجابة للحوادث، مع تبني تقنيات الذكاء الاصطناعي والتعلم الآلي لتحسين قدرات الكشف والتحليل.
- الاستجابة (Response): تشكيل فرق استجابة متخصصة ومدرّبة للتعامل مع الحوادث السيبرانية، ووضع بروتوكولات وإجراءات موحدة للتعامل مع مختلف أنواع التهديدات.

المراقبة والتقييم

لضمان فعالية تنفيذ سياسات الأمن السيبراني، يجب وضع آليات واضحة للمراقبة والتقييم. تشمل مؤشرات الأداء الرئيسية:

1. انخفاض الهجمات السيبرانية الناجحة: قياس عدد الهجمات التي تم صدها بنجاح.
2. تحسين أمن البنية التحتية: تقييم مستوى تأمين الشبكات والأنظمة الرقمية.
3. إنشاء أطر تنظيمية: متابعة تطوير وتفعيل القوانين والسياسات المتعلقة بالأمن السيبراني.

يجب مراجعة الأهداف قصيرة وطويلة الأجل بشكل دوري لضمان مواءمتها مع التهديدات السيبرانية المتطورة. كما يتعين إجراء تقييمات منتظمة لفعالية البرامج والمبادرات، مع إشراك جميع الجهات المعنية لضمان الشفافية والمساءلة.

الخاتمة

تعزيز الأمن السيبراني في ليبيا يمثل خطوة حاسمة نحو تحقيق مستقبل رقمي آمن. من خلال تنفيذ هذا الإطار السياسي، يمكن للبلاد الحد من المخاطر السيبرانية، وحماية بيانات المواطنين، ودعم النمو الرقمي الآمن. تنفيذ هذه السياسات والتوصيات سيسهم بشكل كبير في تحقيق رؤية الاستراتيجية الوطنية لمستقبل رقمي آمن للبلاد.

³ إطار العمل ROAR هو نهج منظم يُستخدم في إدارة المشاريع وتطوير المنظمات، يركز على النتائج والأهداف والإجراءات والمراجعة. يُبرز أهمية تحديد النتائج الواضحة، وضع أهداف محددة، تحديد الإجراءات اللازمة، ومراجعة التقدم بانتظام لضمان التنفيذ الناجح والقدرة على التكيف.



من خلال تبني نهج شامل ومتكامل للأمن السيبراني، ستتمكن ليبيا من بناء بيئة رقمية موثوقة تدعم النمو الاقتصادي، وتحسن جودة الخدمات الحكومية، وتعزز الثقة في التعاملات الإلكترونية. الالتزام بهذه التوصيات هو استثمار في مستقبل البلاد وقدرتها على المنافسة في العصر الرقمي.

موجز سياسة حول الحيز الرقمي من منظور حقوق الإنسان في ليبيا

الملخص التنفيذي

تشهد ليبيا تحولاً بطيئاً نحو الرقمنة بسبب التحديات السياسية والاقتصادية، ولكن مع الاعتماد المتزايد على التقنيات الرقمية، تظهر قضايا حقوق الإنسان بشكل أوضح. من أبرز هذه القضايا: حماية البيانات الشخصية، حقوق الوصول إلى الإنترنت، الرقابة على المحتوى، وتحديات المساواة في الوصول إلى التكنولوجيا.

التوصيات الرئيسية

ثم إعداد هذه التوصيات من قبل مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية، والتي تضم طيفاً واسعاً من أصحاب المصلحة، بما في ذلك الأكاديميين، ممثلي القطاع الخاص، منظمات المجتمع المدني (NGOs)، المحامين والخبراء القانونيين، خبراء التكنولوجيا المستقلين، وعدة مؤسسات حكومية. وتتمثل هذه التوصيات في:

1. تطوير قانون لحماية الحقوق الرقمية.
2. ضمان الوصول المتساوي إلى الإنترنت.
3. حماية حرية التعبير عبر الإنترنت.



4. دعم برامج التثقيف الرقمي للمجموعات المهمشة.

5. تعزيز التعاون الدولي.

المقدمة

في عصر التكنولوجيا الرقمية المتسارع، أصبحت الرقمنة جزءًا لا يتجزأ من الحياة اليومية في ليبيا والعالم. توفر الرقمنة فرصًا للنمو الاقتصادي، وتعزيز الشفافية، وتحسين الخدمات الحكومية، لكنها تطرح أيضًا تحديات جديدة فيما يتعلق بحماية حقوق الإنسان. يتطلب ضمان حقوق الأفراد في الفضاء الرقمي موازنة دقيقة بين التحول الرقمي وحماية الحريات الأساسية مثل الخصوصية، حرية التعبير، والمساواة في الوصول إلى التكنولوجيا.

الأهداف والغايات الاستراتيجية

تهدف هذه السياسة إلى حماية حقوق الإنسان ضمن الحيز الرقمي من خلال:

1. حماية حقوق الإنسان في الفضاء الرقمي من خلال ضمان حرية التعبير، الخصوصية، والوصول العادل إلى التكنولوجيا.
2. تحقيق المساواة في الوصول إلى التكنولوجيا، بحيث يستفيد الجميع من الحيز الرقمي، بما في ذلك الفئات المهمشة والمناطق الريفية.
3. تعزيز الشفافية والمساءلة في استخدام البيانات الشخصية وتطبيقات الذكاء الاصطناعي.
4. تمكين الأفراد والمجتمعات من التفاعل مع العالم الرقمي بأمان، مع ضمان عدم تعرضهم للاستغلال أو التمييز.

التحديات الرئيسية

1. الخصوصية وحماية البيانات: تفتقر ليبيا إلى قوانين شاملة لحماية البيانات، مما يعرض الأفراد لمخاطر تتعلق بإساءة استخدام معلوماتهم الشخصية.
2. التمييز في الوصول إلى التكنولوجيا: تعاني العديد من المناطق الريفية والمهمشة من ضعف في الوصول إلى الإنترنت والتكنولوجيا، مما يوسع الفجوة الرقمية ويزيد من عدم المساواة.
3. الرقابة على الإنترنت وحرية التعبير: يشكل فرض الرقابة على الإنترنت ووسائل التواصل الاجتماعي تهديدًا لحرية التعبير ويحد من قدرة الأفراد على المشاركة في الحياة العامة.
4. الرقمنة والعدالة الاجتماعية: هناك تحديات تتعلق بتوفير الفرص المتكافئة لجميع المواطنين للوصول إلى التكنولوجيا والموارد الرقمية، خاصة للفئات الضعيفة مثل النساء والشباب في المناطق المحرومة.

التوصيات والإجراءات السياسية

تم إعداد هذه التوصيات من قبل مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية، والتي تضم طيفًا واسعًا من أصحاب المصلحة، بما في ذلك الأكاديميين، ممثلي القطاع الخاص، منظمات المجتمع المدني (NGOs)، المحامين والخبراء القانونيين، خبراء التكنولوجيا المستقلين، وعدة مؤسسات حكومية. وتتمثل هذه التوصيات في:

- 1- تطوير إطار قانوني شامل لحماية الحقوق الرقمية: وضع قانون شامل لحماية البيانات يتماشى مع المعايير الدولية.
- 2- ضمان الوصول المتساوي للتكنولوجيا: تنفيذ سياسات لتوفير خدمات الإنترنت لجميع المواطنين، مع التركيز على المناطق الريفية والمهمشة.



- 3- حماية حرية التعبير: وضع تشريعات واضحة لحماية حرية التعبير على الإنترنت والحد من الرقابة غير المبررة.
- 4- تعزيز الوعي والتثقيف الرقمي: إطلاق برامج توعية وطنية حول حقوق الإنسان الرقمية تستهدف الأفراد والمؤسسات.
- 5- التعاون مع المنظمات الدولية: تعزيز التعاون مع المؤسسات الدولية لتحسين الأطر التشريعية والتقنية المتعلقة بالحقوق الرقمية.

المبادرات والسياسات والقوانين الرئيسية المتعلقة بالرقمنة من منظور حقوق الإنسان في ليبيا حتى عام 2024

1. مشروع الحكومة الإلكترونية التي تسعى لرقمنة الخدمات العامة لتسهيل الوصول إليها وتعزيز الشفافية والمساءلة في تقديم الخدمات.
2. السياسة الوطنية للنفاذية الرقمية: تهدف هذه السياسة إلى تعزيز النفاذية الرقمية في ليبيا، مع اتباع توصيات اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا) لدعم صناع السياسات في العالم العربي. هذا يهدف إلى تطوير سياسات وطنية لتعزيز النفاذية الرقمية.
3. قانون مكافحة الجرائم الإلكترونية (قانون رقم 5 لسنة 2022): يحتوي هذا القانون على أحكام لحماية البيانات الشخصية في التعاملات الإلكترونية، ولكن نطاق تطبيقه محدود، ولا يغطي جميع الجوانب المتعلقة بحماية الخصوصية الرقمية وحقوق الإنسان.
4. سياسات الهيئة الوطنية لأمن وسلامة المعلومات (NSA): أصدرت الهيئة مجموعة من السياسات لتعزيز أمن المعلومات، مثل سياسة حماية البيانات، سياسة الاستخدام المقبول، سياسات حماية الشبكات، وسياسة النسخ الاحتياطي. تركز هذه السياسات على حماية المعلومات والأصول الرقمية، لكنها لا تعالج بشكل مباشر مسألة حماية الخصوصية الشخصية وقضايا حقوق الإنسان.

الإطار التنفيذي (ROAR)

يعتمد الإطار التنفيذي (ROAR) على أفضل الممارسات العالمية في مجال الرقمنة، مستلهمًا من إرشادات المنظمات الدولية مثل المعهد الوطني للمعايير والتقنية (NIST) والاتحاد الدولي للاتصالات (ITU). في ظل التحديات المتزايدة التي تواجهها ليبيا في مجال الرقمنة، سواء من منظور حقوق الإنسان أو بسبب نقص البنية التحتية الرقمية المتطورة، يوفر إطار ROAR فرصة لتطوير منظومة وطنية تضمن دمج مبادئ حقوق الإنسان في التحول الرقمي وتعزيز الحماية الرقمية.

ويعتمد الإطار على أربعة ركائز أساسية:

(R)المسؤوليات Responsibilities

- الحكومة: وضع الأطر القانونية والسياسات المتعلقة بالحقوق الرقمية.
- القطاع الخاص: تبني ممارسات شفافة في التعامل مع البيانات واحترام الخصوصية.
- المجتمع المدني: مراقبة وحماية حقوق الإنسان في الفضاء الرقمي وتعزيز الوعي الرقمي بين المواطنين.

(O)الفرص Opportunities

- التحول الرقمي للخدمات العامة: يوفر فرصًا لتحسين الشفافية والعدالة في تقديم الخدمات.
- تعليم رقمي للجميع: إدخال التكنولوجيا في التعليم يمكن أن يساعد في تحسين مهارات الشباب وفتح فرص عمل جديدة.

(A)المساءلة Accountability



- هيئة رقابة رقمية وطنية: لضمان تطبيق القوانين والمعايير المتعلقة بحقوق الإنسان في الفضاء الرقمي.

Risks المخاطر

- الاستغلال الرقمي: بدون إطار قانوني صارم، قد يتم استغلال المواطنين من خلال إساءة استخدام بياناتهم الشخصية.
- الفجوة الرقمية: قد يؤدي عدم توفير التكنولوجيا بشكل متساوٍ إلى تفاقم التهميش الاجتماعي والاقتصادي.

الرصد والتقييم

يعد إطار عمل قوي للرصد والتقييم أمرًا بالغ الأهمية لتتبع تقدم التحول الرقمي في ليبيا. تشمل المؤشرات الرئيسية معدلات الإلمام الرقمي، المساواة في الوصول إلى التكنولوجيا، والامتثال لقوانين الخصوصية. يجب أن تضمن المراجعات الدورية أن الرقمنة تتماشى مع معايير حقوق الإنسان وتلبي احتياجات جميع المواطنين، وخاصة الفئات المهمشة. سيعزز هذا الإطار المساواة والشفافية والتحسين المستمر، مما يساعد ليبيا على تحقيق مستقبل رقمي متوازن وشامل.

الخاتمة

تمثل الرقمنة فرصة حيوية لتعزيز التنمية الاقتصادية والاجتماعية في ليبيا، ولكن يجب تنفيذها مع توفير ضمانات صارمة لحماية حقوق الإنسان. إن اتباع نهج يوازن بين التحول الرقمي وحقوق الأفراد في الفضاء الرقمي سيمكن ليبيا من تحقيق العدالة الرقمية وتعزيز الثقة في التقنيات الحديثة. عبر تنفيذ هذه التوصيات، يمكن للحكومة الليبية تطوير إطار سياسي يحافظ على حقوق الأفراد ويضمن شمولية الوصول الرقمي لجميع المواطنين، مما يساهم في خلق بيئة رقمية آمنة وعادلة ومستدامة.



موجز سياسة حول حماية خصوصية البيانات الشخصية في ليبيا

الملخص التنفيذي

في خضمّ التحول الرقمي الذي تشهده ليبيا، باتت خصوصية البيانات الشخصية ضرورة حتمية لكسب ثقة الجمهور وتحفيز المشاركة الاقتصادية. لذلك، يوصي هذا الموجز السياسي بوضع إطار متكامل لحماية خصوصية البيانات يتوافق مع المعايير الدولية، بما يضمن صون البيانات الشخصية وتعزيز الثقة ودعم نمو الاقتصاد الرقمي في ليبيا.

التوصيات الرئيسية

1. وضع سياسة شاملة: تشكيل لجنة خبراء، تحديد مبادئ حماية البيانات، تنظيم جمع البيانات واستخدامها ونقلها.
2. تعزيز الإطار القانوني: صياغة قانون حماية البيانات، تحديث القوانين الحالية لضمان التوافق.
3. زيادة الوعي العام: إطلاق حملات توعية حول الخصوصية، إدراج مفاهيم الخصوصية في المناهج الدراسية.
4. تعزيز القدرات التقنية: وضع معايير أمن البيانات، تدريب الكوادر على حماية البيانات، تعزيز تقنيات الخصوصية.
5. تعزيز التعاون الدولي: تبني أفضل الممارسات العالمية، الانضمام إلى اتفاقيات حماية البيانات الدولية، تطوير آليات التعاون عبر الحدود.
6. ضمان المراجعة المستمرة: تحديث سياسة الخصوصية بشكل دوري، تقييم فعالية السياسة.

مقدمة

في عصر التحول الرقمي المتسارع، أصبحت حماية البيانات قضية رئيسية للأفراد والمؤسسات والحكومات على حد سواء. ومع تزايد الاتصال العالمي ودمج التقنيات الرقمية في جميع جوانب الحياة اليومية، ارتفع حجم البيانات الشخصية التي يتم إنشاؤها وجمعها ومعالجتها بشكل كبير.

تواجه ليبيا، مثل العديد من الدول النامية، مفترق طرق حاسم في رحلتها الرقمية. بينما تسعى البلاد إلى تحديث بنيتها التحتية واعتماد التقنيات الرقمية، فإنها تواجه الحاجة الملحة إلى إنشاء إطار قانوني وتنظيمي قوي لحماية البيانات. حاليًا، تفتقر ليبيا إلى قانون شامل لحماية البيانات، مما يترك المعلومات الشخصية لمواطنيها عرضة لأنواع مختلفة من سوء الاستخدام والإساءة. لا تؤدي هذه الفجوة التشريعية إلى تعريض الخصوصية الفردية للخطر فحسب، بل تعيق أيضًا قدرة البلاد على المشاركة الكاملة في الاقتصاد الرقمي العالمي، حيث أصبحت معايير حماية البيانات شرطًا أساسيًا للتجارة والتعاون الدولي.

السياق الحالي

- عدم وجود قانون شامل لحماية البيانات: لا تملك ليبيا حاليًا قانونًا وطنيًا شاملاً ينظم جمع البيانات الشخصية واستخدامها وكشفها.
- حماية دستورية محدودة: يضمن الإعلان الدستوري الليبي لعام 2011 الحق في الحياة الخاصة وسرية الاتصالات، لكن هذه الأحكام لا تُقدم تفاصيل كافية بشأن حماية البيانات الشخصية في العصر الرقمي.
- قانون العقوبات الليبي لعام 1953: يُقدم هذا القانون بعض الحماية للخصوصية البدنية والمراسلات الخاصة، لكنه لا يُعالج قضايا البيانات الرقمية.
- قانون رقم (4) لسنة 1990 بشأن النظام الوطني للمعلومات والتوثيق.



- قانون مكافحة الجرائم الإلكترونية (قانون رقم 5 لسنة 2022): يتضمن هذا القانون الجديد أحكامًا تتعلق بحماية البيانات الشخصية في المعاملات الإلكترونية، لكن نطاق تطبيقه محدود.
- سياسات الهيئة الوطنية لأمن وسلامة المعلومات: أصدرت الهيئة الوطنية لأمن وسلامة المعلومات مجموعة شاملة من 27 سياسة وطنية لأمن وسلامة المعلومات تهدف إلى حماية البيانات والأصول الرقمية لجميع أفراد المجتمع والمؤسسات العاملة على الساحة الوطنية. تغطي هذه السياسات جوانب متعددة من أمن المعلومات، بما في ذلك: سياسة حماية البيانات، سياسة الاستخدام المقبول، سياسات المستخدم، سياسة مكافحة الفيروسات، سياسات حماية الشبكات، سياسة التعامل مع الأطراف الثالثة، سياسة النسخ الاحتياطي، سياسة الأمان المادي

الأهداف والغايات الاستراتيجية

- تهدف سياسة خصوصية البيانات إلى:
- 1. حماية حقوق المواطنين في بياناتهم الشخصية.
- 2. إنشاء إطار قانوني لخصوصية البيانات.
- 3. تعزيز الثقة العامة في المعاملات الرقمية.
- 4. دعم مشاركة البيانات واستخدامها بشكل آمن.

التحديات الرئيسية

1. ضعف الوعي بحقوق البيانات: يفتقر العديد من المواطنين الليبيين إلى الوعي بحقوقهم المتعلقة بالبيانات الشخصية، مما يجعلهم عرضة لانتهاكات الخصوصية.
2. نقص الإجراءات الأمنية: تفتقر العديد من المؤسسات الليبية، سواء العامة أو الخاصة، إلى إجراءات أمنية كافية لحماية البيانات الشخصية.
3. غياب الإطار التشريعي الشامل: إن غياب قانون شامل لحماية البيانات الشخصية في ليبيا يخلق بيئة قانونية غير مستقرة، ويفتح الباب أمام إساءة استخدام البيانات من قبل مختلف الجهات، مما يهدد الحقوق والحريات الأساسية للأفراد.
4. عقبات أمام ممارسة حقوق البيانات: يواجه الأفراد الليبيون صعوبات كبيرة في ممارسة حقوقهم المتعلقة بالبيانات الشخصية، مثل الحق في الوصول إلى البيانات، والحق في تصحيحها، والحق في الاعتراض على معالجتها، وذلك بسبب غياب آليات واضحة وفعالة لتنفيذ هذه الحقوق.

التوصيات لتأسيس سياسة وطنية للخصوصية

تم إعداد هذه التوصيات من قبل مجموعة العمل المتخصصة في إعادة صياغة السياسات العامة الرقمية، والتي تضم طيفًا واسعًا من أصحاب المصلحة، بما في ذلك الأكاديميين، ممثلي القطاع الخاص، منظمات المجتمع المدني، المحامين والخبراء القانونيين، خبراء التكنولوجيا المستقلين، وعدة مؤسسات حكومية. وتتمثل هذه التوصيات في:

1. صياغة وإقرار سياسة وطنية شاملة للخصوصية:
- تشكيل لجنة وطنية متخصصة لصياغة السياسة بمشاركة خبراء قانونيين وتقنيين.
- تحديد الاحتياجات والمبادئ الأساسية لحماية البيانات الشخصية في ليبيا.
- وضع إطار عمل لتنظيم جمع البيانات الشخصية، واستخدامها، وتخزينها ونقلها.



- تعريف حقوق الأفراد في الخصوصية والية التحكم ببياناتهم الشخصية وتحديد الاشخاص والجهات الاعتبارية المخولين بالوصول للبيانات.

2. تطوير الإطار القانوني:

- صياغة مشروع قانون شامل لحماية البيانات يستند إلى السياسة الوطنية للخصوصية.
- مراجعة وتحديث القوانين القائمة لضمان توافقها مع سياسة الخصوصية الجديدة.

3. بناء الوعي العام:

- إطلاق حملة وطنية لتعريف المواطنين بأهمية الخصوصية الرقمية وحقوقهم الجديدة.
- دمج مفاهيم حماية البيانات الشخصية في المناهج التعليمية.

4. تعزيز القدرات التقنية:

- وضع معايير وطنية لأمن البيانات وحمايتها.
- تدريب الكوادر الحكومية والخاصة على تطبيق أفضل ممارسات حماية البيانات.
- تشجيع تطوير واستخدام تقنيات حديثة لحماية الخصوصية.

5. التعاون الدولي:

- دراسة أفضل الممارسات العالمية في مجال سياسات الخصوصية.
- السعي للانضمام إلى الاتفاقيات الدولية المتعلقة بحماية البيانات.
- تطوير آليات للتعاون عبر الحدود في قضايا حماية البيانات.

6. المراجعة والتحديث المستمر:

- وضع آلية لمراجعة وتحديث السياسة الوطنية للخصوصية بشكل دوري.
- إجراء تقييمات منتظمة لفعالية السياسة وتأثيرها على حماية حقوق المواطنين.

مواءمة سياسة الخصوصية الوطنية مع مبادئ ROAM الخاصة باليونسكو

بالتوافق مع مبادئ اليونسكو لحرية الإنترنت (ROAM) التي تشمل الحقوق والانفتاح والوصول والمشاركة المتعددة الأطراف، سوف تهدف سياسة الخصوصية الوطنية الجديدة إلى:

- حماية حقوق الأفراد في الخصوصية.
- ضمان الشفافية في ممارسات جمع البيانات واستخدامها.
- دعم وصول الجميع إلى الإنترنت وتعزيز الوعي الرقمي.
- تشجيع المشاركة المتعددة الأطراف في صياغة وتنفيذ سياسة الخصوصية.

الرصد والتقييم

سيقوم إطار عمل قوي للرصد والتقييم بتتبع التقدم باستخدام مؤشرات مثل امتثال حماية البيانات، مستويات الوعي العام، وحوادث انتهاكات البيانات. ستقوم المراجعات الدورية بتقييم فعالية السياسة في تحقيق أهداف مثل الإصلاح القانوني، بناء



الخاتمة

إن تأسيس سياسة وطنية شاملة للخصوصية في ليبيا يعد خطوة حاسمة نحو حماية حقوق المواطنين الرقمية وتعزيز مكانة البلاد في العصر الرقمي. يتطلب تنفيذ هذه التوصيات التزامًا سياسيًا قويًا وتعاونًا بين مختلف الجهات المعنية. من شأن هذه الجهود أن تضع الأساس لبيئة رقمية آمنة وموثوقة في ليبيا، تحمي خصوصية المواطنين وتدعم التنمية الاقتصادية والاجتماعية.



الملاحظات الختامية

تُعدّ هذه الموجزات وثائق ديناميكية قابلة للتطوير والتحسين بمرور الوقت. يمكن مراجعة السياسات والإجراءات المقترحة وتحديثها باستمرار بناءً على التغيرات في البيئة التكنولوجية والسياسية والاقتصادية. من خلال تنفيذ هذه الإجراءات الاستراتيجية، تستطيع ليبيا بناء الثقة في أنظمتها الرقمية وتمكين مواطنيها، وتبوء مكانة رائدة في الاقتصاد الرقمي إقليمياً. وبالالتزام المشترك بالابتكار والمرونة، تتمكن الدولة من تحقيق الفوائد الكاملة للرقمنة مع حماية شعبها وبنيتها التحتية.

المنهجية

- النهج الاستشاري: إجراء مشاورات موسعة مع عدة جهات حكومية والمجتمع المدني والقطاع الخاص والأوساط الأكاديمية والأفراد ذوي الإعاقة.
- مراجعة الأدبيات والتحليل المقارن: تحليل معمق لأفضل الممارسات العالمية والسياسات الإقليمية.
- استشارات الخبراء وورش العمل: تنظيم ورش عمل وحلقات نقاش مع الخبراء لجمع الرؤى وتحسين التوصيات السياسية.

البيانات

- الاستطلاعات والمقابلات: تم تنفيذها لجمع بيانات كمية ونوعية من الأطراف المعنية.
- تحليل البيانات: استخدام أدوات تحليل البيانات لتحديد وتطوير توصيات سياسية قائمة على أدلة وأسس علمية.
- رسم أصحاب المصلحة: تحديد أصحاب المصلحة المعنيين لضمان مشاركة شاملة وجمع الآراء.

الملحق 1: الموارد والأدوات الداعمة

- (نموذج) [ROAR](#) المرونة، القابلية للملاحظة، الأتمتة، الاستجابة: إطار لتقييم وتعزيز المرونة الرقمية، مع التركيز على المرونة والقابلية للملاحظة والأتمتة والاستجابة. تعرّف على المزيد.
- منصة: [Mural](#) دعمت ورش العمل على منصة Mural التعاون المرئي لإصلاحات الحقوق الرقمية والأمن السيبراني.
- مدونات توثق رحلة عنبر للتنمية
- سلسلة مدونات تُفصّل عملية وضع الموجز السياساتي، بما في ذلك التحديات والإنجازات. قراءة المدونات.
- تم استخدام أداة تقييم تأثير الإنترنت (IIAT) في تحليل وتقييم تأثير عدد من التشريعات والسياسات الليبية على بيئة الإنترنت، لا سيما فيما يتعلق بجوانب الانفتاح، الوصول، الخصوصية، والأمن. وقد شملت التقييمات ما يلي:
 - موجز تأثير الإنترنت حول قانون المعاملات الإلكترونية رقم 6 لسنة 2022
 - موجز تأثير الإنترنت حول قانون مكافحة الجرائم الإلكترونية رقم 5 لسنة 2022
 - موجز تأثير الإنترنت حول قانون الاتصالات رقم 22 لسنة 2010
 - موجز تأثير الإنترنت حول قانون نظام المعلومات والتوثيق الوطني رقم 4 لسنة 1990

حقوق النشر والمعلومات

- مبادرة أنير ©2024



- الإصدار 1:1. أكتوبر 2024
- التحديثات: يتم مراجعتها نصف سنوياً
- تصميم المحتوى: أسامة منصور، خير سياسات - بالشراكة مع مبادرة أنير ومجتمع الإنترنت - ليبيا

للتواصل:

✉ xxx@anir.ly | 🌐 www.anir.ly | ☎ +218 xxxxxxx