المملكة المغربية

البرلمان

مجلس المستشارين

مشروع قانون

رقم 52.21 يوافق بموجبه على اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المعتمدة بمالابو(غينيا الاستوائية) في 27 يونيو 2014

(كما وافق عليه مجلس المستشارين في 18 يناير 2022)

نسخة مطابقة لأصل النص
كما وافق عليه مجلس المستشارين

النعم ميارة
رئيس مجلس المستشارين

مشروع قانون رقم 52.21
يوافق بموجبه على اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المعتمدة بمالابو (غينيا الاستوائية) في 27 يونيو 2014

مادة فريدة

يوافق على اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي، المعتمدة بمالابو (غينيا الاستوائية) في 27 يونيو 2014، مع مراعاة الإعلان التفسيري الذي قدمته المملكة المغربية في شأنها.

*

* *

اتفاقية الاتحاد الأفريقي بشأن أمن الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي

الديباجة

إن الدول الأعضاء في الإتحاد الأفريقي:

إذ تسترشد بالقانون التأسيسي للإتحاد الأفريقي المعتمد في عام 2000

وإذ تأخذ في الإعتبار أن هذة الاتفاقية المتعلقة باعتماد إطار قانوني **للأمن في الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي تتكفل** بالالتزامات الحالية للدول الأعضاء في الإتحاد الإفريقي على المستويات الإقليمية الفرعية والإقليمية والدولية لبناء مجتمع المعلومات.

وإذ تشير إلى أنها تهدف إلى محاولة تحديد الأهداف والتوجيهات الرئيسية لمجتمع المعلومات في إفريقيا وتعزيز التشريعات والأنظمة الحالية الخاصة بتكنولوجيات المعلومات والإتصالات للدول الأعضاء والمجموعات الإقتصادية الإقليمية؛

وتؤكد مجددا تمسك الدول الأعضاء في الإتحاد الأفريقي بالحريات الأساسية وحقوق الإنسان والشعوب الواردة في الإعلانات والإتفاقيات وغيرها من الصكوك المعتمدة في إطار الإتحاد الأفريقي والأمم المتحدة؛

وإذ تأخذ في الإعتبار أن إنشاء إطار معياري حول الأمن في الفضاء الإ لكتروني وحماية البيانات ذات الطابع الشخصي يراعي متطلبات إحترام حقوق المواطنين الأساسية المكفولة بموجب النصوص الأساسية للقانون المحلي وبموجب الإتفاقيات والمعاهدات الدولية المتصلة بحقوق الإنسان ولا سيما الميثاق الأفريقي لحقوق الإنسان والشعوب.

وإذ تعرب عن إقتناعها بضرورة تعبئة كافة الأطراف الفاعلة العامة والخاصة (الحكومات والمجتمعات المحلية ومؤسسات القطاع الخاص ومنظمات المجتمع المدني ووسائل الإعلام ومؤسسات التدريب والبحث، الخ) نحو تحقيق أمن الفضاء الإلكتروني؛

وإذ تؤكد مجددا مبادئ المبادرة الأفريقية لمجتمع المعلومات وخطة العمل الإقليمية الإفريقية لإقتصاد المعرفة؛

وإذ تعي أن الإتفاقية تستهدف إلي تنظيم مجال تكنولوجي متطور بشكل خاص، وسعيا إلى الإستجابة للتطلعات الملحة للعديد من الأطراف الفاعلة التي غالباً ما تتعارض مصالحها، تحدد **هذه الإتفاقية** قواعد الأمن الضرورية لإنشاء فضاء رقمي موثوق به للمعاملات الإلكترونية وحماية البيانات ذات الطابع الشخصي ومكافحة الجريمة الإلكترونية؛

وإذ تضع في الحسبان أن التحديات الرئيسية التي تواجه تنمية التجارة الإلكترونية في إفريقيا مرتبطة بمشاكل أمنية، ومنها على وجه الخصوص:

أ) أوجه القصور المؤثرة في تنظيم الإعتراف القانوني بالإتصالات البيانية والتوقيع الإلكتروني؛

ب) عدم وجود قواعد قانونية محددة تحمي المستهلكين وحقوق الملكية الفكرية والبيانات ذات الطابع الشخصي وأنظمة المعلومات؛

ج) عدم وجود تشريعات متعلقة بالخدمات الإلكترونية والعمل عن بُعد؛

د) تطبيق تقنيات إلكترونية على الأعمال التجارية والإدارية؛

هـ) الأدلة الموثوق بها الناجمة عن التقنيات الرقمية (الطابع الزمني، الشهادة، إلخ)؛

و) القواعد المطبقة على أجهزة وخدمات التشفير ؛

ز) الرقابة على الإعلانات عبر الإنترنت ؛

ح) عدم وجود تشريعات مالية وجمركية ملائمة للتجارة الإلكترونية؛

وإذ تعرب عن قناعتها بأن هذه الملاحظات تبرر الدعوة إلى وضع إطار معياري ملائم يتناسق مع البيئة القانونية والثقافية والاقتصادية والاجتماعية الإفريقية؛ وبأن هذة الاتفاقية تهدف بالتالي إلى كفالة الأمن والإطار القانوني الضروريين لظهور إقتصاد المعرفة في إفريقيا؛

وإذ تؤكد من جانب آخر أن حماية البيانات ذات الطابع الشخصي والحياة الخاصة تشكل تحدياً رئيسياً لمجتمع المعلومات بالنسبة للسلطات الحكومية والأطراف المعنية الأخرى على حدٍ سواء؛ وأن هذه الحماية تقتضي توازنا بين إستخدام تكنولوجيا المعلومات والإتصالات وحماية الحياة الخاصة للمواطنين في نشاطاتهم اليومية أوالمهنية مع ضمان حرية تداول المعلومات؛

وإذ يساورها القلق جراء الحاجة الماسة إلى وضع آلية كفيلة بالتصدي للأخطار الناجمة عن إستخدام البيانات الإ لكترونية والملفات الخاصة بالأفراد حرصا على إحترام الخصوصية والحريات مع تعزيز ترويج وتطوير تكنولوجيا المعلومات والإتصالات في الدول الأعضاء في الإتحاد الإفريقي؛

وإذ تأخذ في الإعتبار أن ما تتطلع إليه هذه الإتفاقية هو الإستجابة للإحتياجات المتمثلة في وضع تشريعات متناسقة، في مجال الأمن الإلكتروني بالدول الأعضاء في الإتحاد الإفريقي وأنها تستهدف إلي وضع آلية في كل دولة طرف، قادرة علي مكافحة الإنتهاكات للخصوصية، والتي قد تنشأ عن جمع ومعالجة ونقل وتخزين وإستخدام بيانات ذات طابع شخصي؛ وأنها تضمن، من خلال إقتراح نوع من الدعم المؤسسي، أن تحترم أية معالجة، بأي شكل كانت، الحريات والحقوق الأساسية للأفراد مع الأخذ بعين الإعتبار في نفس الوقت صلاحيات الدول وحقوق المجتمعات المحلية ومصالح مؤسسات الأعمال التجارية؛ وكذلك مع مراعاة أفضل الممارسات المعترف بها على الصعيد الدولي؛

وإذ تأخذ في الإعتبار أن الحماية الجنائية لمنظومة القيم لمجتمع المعلومات ضرورة حتمية تمليها إعتبارات أمنية؛ وأنها تتجلى في المقام الأول بسبب الحاجة إلى التشريعات الجنائية المناسبة في مكافحة الجريمة الإلكترونية بشكل عام، وغسل الأموال على وجه الخصوص؛

وإذ تدرك أنه من الضروري، في ظل إنتشار الجريمة الإلكترونية التي تشكل تهديداً حقيقياً لأمن شبكات الحاسوب وتطور مجتمع المعلومات في إفريقيا، تحديد توجيهات عامة لإستراتيجية مكافحة الجريمة الإلكترونية في الدول الأعضاء في الاتحاد الإفريقي، مع الأخذ في الإعتبار إلتزاماتها الحالية على المستويات الإقليمية الفرعية والإقليمية والدولية؛

وإذ تأخذ في الإعتبار أن هذة الاتفاقية تهدف، من حيث القانون الجنائي الموضوعي، إلى تحديث أدوات قمع الجريمة الإلكترونية من خلال وضع سياسات لإعتماد جرائم جديدة خاصة بتكنولوجيا المعلومات والإتصالات وموائمة نظام العقوبات الموجود فعلياً في الدول الأعضاء مع المناخ التكنولوجي الحديث وبيئة تكنولوجيا المعلومات والإتصالات؛

وإذ تأخذ في الإعتبار أيضاً أن الإتفاقية، من حيث القانون الجنائي الإجرائي، تحدد من جهة، ، آلية لتكييف الإجراءات القياسية الخاصة بتكنولوجيا المعلومات والإتصالات، وتوضح من جهة أخرى شروط وضع إجراءات خاصة بالجريمة الإلكترونية؛

وإذ تشير إلى بيب اعلان المؤتمر (ASSEMBLY/AU/DECL.1(XIV الصادر عن الدورة الرابعة عشر لمؤتمر رؤساء دول وحكومات الإتحاد الإفريقي بشأن تكنولوجيا المعلومات والإتصالات في أفريقيا: التحديات والآفاق المستقبلية للتنمية، المنعقدة في أديس أبابا، إثيوبيا من 31 يناير إلى 2 فبراير 2010؛

وإذ تأخذ في الإعتبار إعلان أوليفر تامبو الذي إعتمده مؤتمر الإتحاد الإفريقي الإستثنائي للوزراء المسؤولين عن تكنولوجيا المعلومات والإتصالات المنعقد في جنوب افريقيا بجوهانسبيرغ في 5 نوفمبر 2009؛

وإذ تذكر بأحكام كل من إعلان أبيدجان المعتمد في 22 فبراير 2012، وإعلان أديس أبابا المعتمد في 22 يونيو 2012 حول مواءمة تشريعات الفضاء الإلكتروني فى إفريقيا.

إتفقت على ما يلي:

المادة 1: التعريفات

لأغراض هذه الإتفاقية، يتم التعريف بمختلف التعبيرات على النحو التالي:

الاتحاد الافريقي : /الإتحاد الإفريقي

المواد الإباحية للأطفال: تعنى أي تمثيل بصري لسلوك جنسي صريح، بما في ذلك أي صورة أو فيلم أو فيديو أو صورة بالحاسوب سواءً أنتجت بوسائل إلكترونية أو ميكانيكية أو وسائل أخرى، حيث :

(أ) يشمل إنتاج هذا التمثيل البصري إستعمال قاصر؛

(ب) يتعلق هذا التمثيل البصري بصورة رقمية أو صورة بالحاسوب أو صورة تمت بالحاسوب حيث يشارك قاصر في نشاط جنسي صريح أو عند ما يتم إنتاج إستعمال صور أعضائه التناسلية لأغراض جنسية بشكل أساسي واستغلالها بعلم الطفل أو بدون علمه؛

(ج) تم إنشاء هذا التمثيل البصري أو تكييفه أو تعديله ليشارك قاصر في نشاط جنسي صريح.

مدونة قواعد السلوك: وتعني مجموعة القواعد التي يضعها مسؤول المعالجة بغية لأستعمال صحيح لموارد تكنولوجيا المعلومات والشبكات والإتصالات الإلكترونية للهيكل المعني والمعتمد من قبل سلطة الحماية.

المفوضية : تعني مفوضية الإتحاد الأفريقي

الإتصال مع الجمهور بواسطة وسائل إلكترونية: ويعني جميع ما يتم تعميمه، من خلال إجراء إتصال إلكتروني، على الجمهور أو على شرائح معينة من الجمهور من علامات أو إشارات أو مواد خطية أو صور أو أصوات أو رسائل أياً كان نوعها دون أن تتصف بصفة مراسلات خاصة.

نظام الحاسوب: يعني جهازا إلكترونيا، مغناطيسيا، بصريا، كهروكيمياويا، أو أي جهاز آخر عريض النطاق معزول أو مترابط يؤدي وظيفة تخزين البيانات أو إقامة الإتصالات. وتكون هذه الإتصالات مرتبطة بصورة مباشرة بجهاز أو أجهزة أخرى أو تعمل بالإشتراك معها.

البيانات المحوسبة: وتعني أي عرض لحقائق أو معلومات أو مفاهيم على شكل ملائم للمعالجة بالحاسوب.

موافقة الشخص المعني: وتعني إظهار رغبة بحرية صريحة وواضحة ومحددة ومدروسة يقبل بموجبها الشخص المعني أو ممثله القانوني أو القضائي بمعالجة بياناته الشخصية يدوياً أو إلكترونياً.

هذه الإتفاقية: تعني إتفاقية الإتحاد الأفريقي حول الأمن في الفضاء الإلكتروني وحماية البيانات ذات الطابع الشخصي.

البنية التحتية الحيوية للإنترنت/تكنولوجيا المعلومات والإتصالات: تعني الهياكل الأساسية لتكنولوجيا المعلومات والإتصالات / الإنترنت التي تعد حيوية للخدمات الرئيسية من أجل السلامة العامة والإستقرار الإقتصادي والأمن الوطني والإستقرار الدولي ولإستدامة وإستعادة نشاط الإنترنت.

(نشاط)علم التشفير: ويعني جميع النشاطات التي تهدف إلى إنتاج أو إستعمال أو إستيراد أو تصدير أو تسويق أدوات التشفير.

علم التشفير: ويعني العلم المتعلق بحماية وتأمين المعلومات خصوصاً لغرض ضمان السرية والتوثيق والسلامة وعدم التنصل منها؛

(ادوات) علم التشفير: وتعني مجموعة من الأدوات العلمية والفنية (معدات أو برمجيات) التي تسمح بالتشفير و/أو فك التشفير؛

(خدمات) علم التشفير: وتعني أي عملية تهدف إلى تنفيذ طرق التشفير لحساب شخصي أو لحساب شخص آخر؛

مقدم خدمات علم التشفير: يعني أي شخص طبيعي أو معنوي يقدم خدمات علم التشفير؛

الضرر: ويعني أي مساس بسلامة وتوفر البيانات أو البرنامج أو النظام أو المعلومات؛

المسؤول عن معالجة البيانات: يعني أي شخص طبيعي أو معنوي عام أو خاص أو أي هيئة أو جمعية أخرى تقرر بمفردها أو مع آخرين جمع ومعالجة بيانات ذات طابع شخصي وتحدد أهداف هذه المعالجة؛

الشخص المعني بالبيانات: يعني أي شخص طبيعي يكون محل معالجة البيانات ذات الطابع الشخصي؛

التسويق المباشر: يعني إرسال أي رسالة تستهدف بشكل مباشر أو غير مباشر ترويج سلع وخدمات أو صورة شخص يبيع السلع أو يقدم الخدمات، وتستهدف أيضا إلتماسا منفذا بواسطة رسالة، أيا كانت دعامتها أوطبيعتها، تجارية كانت أم سياسية أو خيرية أو موجهة نحو الترويج المباشر أوغير المباشر للسلع والخدمات أو صورة شخص يبيع سلعا أو يقدم خدمات؛

الجريمة المزدوجة(ازدواجية التجريم): ويقصد بها أن تكون الجريمة معاقبا عليها فى البلد الذي تم فيه إعتقال المشتبه به وأيضا في البلد المطالب بتسليمه أو نقله إليه؛

الإتصـال الإلكترونـي: ويعنـي أي نقل للعلامـات أو الإشارات أو المـواد الخطيـة أو الصـور أو الأصوات أو الرسائل أياً كانت طبيعتها إلى الجمهور أو إلى شريحة من الجمهور بوسائل إتصالات إلكترونية أو مغنطيسية؛

التجارة الإلكترونية: وتعني أي عملا من أعمال عرض وبيع أو توفير السلع والخدمات عبر أنظمة الكمبيوتر وشبكات الإتصالات مثل الإنترنت أو أية شبكة أخرى تستخدم وسائط الإعلام الإلكترونية والبصرية أو وسائل إعلام أخرى لتبادل المعلومات عن بعد؛

البريد الإلكتروني: ويعني أي رسالة فى شكل نص أو صوت أو صورة يتم إرسالها بواسطة شبكة إتصالات عامة وتخزينها في خادم هذة الشبكة أو في المعدات الطرفية المرسل إليها إلى أن يتم إستلامها؛

التوقيع الإليكتروني: يعني بيانات في شكل إلكتروني مرفقة أو مرتبطة منطقياً ببيانات إلكترونية أخرى وتستخدم كوسيلة تعريف وإثبات؛

الجهاز الإلكتروني للتحقق من التوقيع: يعني مجموعة من البرمجيات أو الأجهزة التي تسمح بالتحقق من التوقيع الإ لكتروني؛

الجهاز الإلكتروني لإنشاء التوقيع: يعني مجموعة من البرمجيات أو الأجهزة التي تسمح بإنشاء التوقيع الإلكتروني؛

التشفير: ويعني كل الطرق المتمثلة في تحويل البيانات الرقمية إلى شكل غير مقروء بإستعمال أدوات التشفير؛

تجاوز النفاذ المسموح به: ويعني النفاذ إلى نظام معلومات وإستعمال هذا النفاذ للحصول على معلومات أو تغييرها في جزء من الحاسوب غير مسموح للفرد بالنفاذ إليه؛

البيانات الصحية: وتعني جميع المعلومات المتصلة بالحالة الجسدية أو العقلية للشخص المعني، بما فيها البيانات الوراثية الآنفة الذكر أعلاه؛

الإتصالات الإلكترونية غير المباشرة: وتعني أي رسالة نصية أو صوت أو صورة مرسلة بواسطة شبكة إتصالات إلكترونية تكون مخزنة في الشبكة أو في الجهاز الطرفي للمتلقي إلى حين الإطلاع عليها؛

المعلومات: تعني أي عنصر من عناصر المعرفة يمكن عرضه بواسطة أجهزة من أجل إستعمالها أو حفظها أو معالجتها أو نقلها. ويمكن أن تكون المعلومات على شكل خطي أو صوتي أو بصري أو رقمي أو أشكال أخرى؛

الربط بين البيانات ذات الطابع الشخصي: يعني أي آلية ربط متمثلة في الربط بين بيانات تمت معالجتها لبلوغ هدف محدد وبيانات أخرى معالجة لأهداف مشابهة أو غير مشابهة أو مترابطة بواسطة مسؤول أو أكثر عن المعالجة؛

وسائل الدفع الإلكتروني: تعني الوسائل التي يتمكن بها حامل السند من إجراء عمليات دفع إلكترونية عبر الإنترنت؛

الدولة العضو(أو الدول الأعضاء): تعني الدولة أو الدول الأعضاء في الإتحاد الأفريقي؛

الطفل أو القاصر: يعني أي شخص يقل عمره عن 18 سنة بمقتضى الميثاق الإفريقي لحقوق الطفل ورفاهيته وإتفاقية الأمم المتحدة لحقوق الطفل على التوالي؛

البيانات ذات الطابع الشخصي: وتعني أي معلومات متصلة بشخص طبيعي محدد أو قابل للتحديد بشكل مباشر أو غير مباشر بالإشارة إلى رقم هويته أو إلى عامل واحد أو أكثر محدد لهويته الطبيعية أو الميكولوجية أو الذهنية أو الإقتصادية أو الثقافية أو الإجتماعية؛

ملف البيانات ذات الطابع الشخصي: ويعني كل مجموعة مهيكلة من البيانات التي يمكن الوصول إليها وفق معايير محددة بغض النظر عما إذا كانت هذه البيانات مركزية أو غير مركزية أو موزعة وظيفياً أو جغرافياً؛

معالجة البيانات ذات الطابع الشخصي: وتعني أي عملية أو مجموعة عمليات تجري علي بيانات شخصية بمساعدة أو بدون مساعدة طرق آلية مثل جمع وتسجيل وتنظيم وحفظ وتكييف وتعديل واستخلاص وحماية ونسخ واستشارة واستعمال والكشف من خلال الإرسال ونشر أو أي شكل آخر من أشكال الإتاحة عن طريق المحاذاة أو الربط والقفل، بالإضافة إلى تشفير وحذف وإتلاف بيانات شخصية؛

العنصرية وكراهية الأجانب في تكنولوجيات المعلومات والإتصالات: تعنى أي مادة خطية أو صورة أو أي تمثيل آخر لأفكار أو نظريات تؤيد أو تشجع أو تحرض على الكراهية أو التمييز العنصري أو العنف ضد أي شخص أو مجموعة أشخاص بسبب العرق أو اللون أو السلالة أو الأصل الوطني أو العرقي أو الدين؛

المستفيد من معالجة البيانات: ويعني أي شخص مؤهل لتلقي هذه البيانات غير الشخص المعني، المسؤول عن معالجة البيانات، والمقاول الفرعي والأشخاص المكلفين بسبب وظائفهم بمعالجة البيانات؛

الإتفاقيات السرية: وتعني الرموز غير المعلنة المطلوبة لتنفيذ وسائل أو خدمات علم التشفير لإجراء عمليات الترميز أو فك ترميزها؛

البيانات الحساسة: وتعني جميع البيانات ذات الطابع الشخصي المتصلة بالآراء والأنشطة الدينية والفلسفية والسياسية والنقابية، بالإضافة إلى الحياة الجنسية والعرقية والصحية والتدابير الإجتماعية والقضايا والدعاوى القانونية والعقوبات الجزائية أو الإدارية.

الدولة الطرف (أو الدول الأطراف): وتعني الدولة العضو/الدول الأعضاء التي صدقت على هذه الإتفاقية أو إنضمت إليها؛

المقاول الفرعي: يعني أي شخص طبيعي أو معنوي عام أو خاص أو أي منظمة أو جمعية تقوم بمعالجة البيانات بالنيابة عن مسؤول معالجة البيانات؛

الطرف الثالث: يعني أي شخص طبيعي أو معنوي، عام أو خاص، أو أي سلطة عامة، وكالة أو هيئة غير الشخص المعني، المسؤول عن معالجة البيانات، المقاول الفرعي والأشخاص الذين هم تحت السلطة المباشرة للمسؤول عن معالجة البيانات أو المقاول الفرعي، هؤلاء لهم صلاحية معالجة البيانات؛

الفصل 1

المعاملات الإلكترونية

القسم 1 : التجارة الإلكترونية

المادة 2

مجال تطبيق التجارة الإلكترونية

1. على الدول الأعضاء ضمان حرية ممارسة أنشطة التجارة الإلكترونية في جميع الدول الأطراف المصدقة على هذه الإتفاقية أو المنضمة إليها باستثناء:

أ) المقامرة حتى التي تتخذ شكل المراهنة او اليانصيب المصرح بهما قانونيا؛

ب) أنشطة التمثيل والمساعدة القانونية؛

ج) الأنشطة التي يمارسها كاتبو العدل أو السلطات المماثلة تطبيقا للنصوص القانونية المعمول بها؛

2 . دون المساس بإلتزامات معلوماتية أخرى محددة في النصوص التشريعية والتنظيمية السارية المفعول في الدول الأعضاء في الإتحاد الإفريقي، يتعين على الدول الاطراف ضمان أن يقوم أي شخص يمارس أنشطة التجارة الالكترونية بتزويد من تقدم لهم السلع والخدمات، خدمات الوصول بطريقة سهلة ومباشرة ومستمرة من خلال إستعمال معايير مفتوحة فيما يتعلق بالمعلومات التالية:

أ) في حال مشاركة شخص طبيعي، يتعين على المزود ذكر إسمه أو إسم شركته، في حال وجود شخص معنوي ورأسماله ورقم تسجيله في سجل الشركات أو الجمعيات؛

ب) العنوان الكامل لمكان المؤسسة وعنوان البريد الإلكتروني ورقم الهاتف؛

ج) رقم التسجيل ورأس المال المساهم ومقر الشركة الرئيسي إذا كان الشخص خاضعاً لإجراءات التسجيل المحلية أو التسجيل في دليل الشركات الوطنية؛

د) الرقم الضريبي إذا كان الشخص خاضعاً للضرائب؛

هـ) اذا كان الشخص خاضعا عند ممارسة نشاطه لنظام ترخيص، يتعين ذكر إسم وعنوان الجهة المرخصة ورقم الترخيص؛

و) إذا كان الشخص عضواً في مهنة مقننة وخاضعة للتنظيم، يتعين ذكر القواعد المهنية المطبقة ومنصبه المهني والدولة الطرف التي منح فيها الترخيص بمزاولة المهنة بالإضافة إلى اسم الجهة المهنية المسجل لديها؛

3. على أي شخص طبيعي أو معنوي يمارس أنشطة التجارة الإلكترونية، حتى في حالة عدم وجود عروض تعاقدية وبمجرد إعلان سعر لهذه الأنشطة، أن يذكر هذا السعر بوضوح ودون لبس، لا سيما إذا اشتمل السعر على ضرائب وأجور التسليم وغيرها من الرسوم.

المادة 3

المسؤولية التعاقدية لمزود السلع والخدمات عن طريق الوسائل الإلكترونية

تخضع أنشطة التجارة الالكترونية لقانون الدولة الطرف التى يوجد فى إقليمها الشخص الممارس لهذه الأنشطة، رهنا للنية المشتركة التي يعبر عنها هذا الشخص ومتلقي السلع أو الخدمات.

المادة 4

الدعاية بوسائل إلكترونية

1. مع عدم المساس بالمادة 3، فإن أي عمل دعائي بغض النظر عن شكله، ويمكن الوصول إليه عن طريق خدمات الإتصالات عبر الإنترنت، يجب أن يكون محدد بوضوح وكما ينبغي. و يجب أن يحدد الشخص الطبيعي أو المعنوى الذى تتم تلك الدعاية لحسابه.

2. يجب أن تكون شروط إمكانية الاستفادة من العروض الترويجية وكذلك شروط المشاركة في المنافسات أو الألعاب الترويجية، إذا قدمت هذه العروض والمنافسات والألعاب عبر الإنترنت، واضحة وبدون لبس وسهل الوصول إليها.

3. تلتزم الدول الأطراف في الإتحاد الإفريقي بحظر التسويق المباشر الذى يتم عبر أي شكل من أشكال الإتصال غير المباشر من خلال إستعمال بيانات لشخص طبيعي، بأي شكل من الأشكال، لم يوافق مسبقاً على تلقي هذا التسويق المباشر عن طريق الوسائل المذكورة آنفا.

4. على الرغم من أحكام المادة 2.4 يرخص بالتسويق المباشر بوسائل إلكترونية فى الحالات التالية:

أ) إذا تم الحصول على البيانات ذات الطابع الشخصي الخاصة بالمرسل إليه منه مباشرة؛

ب) إذا وافق المتلقي على إتصال شركاء التسويق؛

ج) إذا تعلق التسويق المباشر بمنتجات أو خدمات مشابهة من نفس الشخص الطبيعى أو المعنوي.

5. تلتزم الدول الأطراف بحظر إرسال رسائل، لغرض التسويق المباشر، عبر أي شكل من أشكال الإتصال الإلكتروني غير المباشر، دون ذكر البيانات الصحيحة التى يمكن أن يرسل إليها المرسل إليه طلباً بإيقاف هذه الإتصالات دون تحمل أي تكاليف غير تلك الناجمة عن إرسال طلب الإيقاف المذكور.

6. تلتزم الدول الأطراف بحظر إخفاء هوية الشخص الذي صدر بإسمه الإعلان الذي يمكن الوصول إليه عن طريق خدمات الإتصال عبر الإنترنت.

القسم 2 : الإلتزامات التعاهدية في شكل إلكتروني

المادة 5

العقود الإلكترونية

1. المعلومات المطلوبة لإبرام عقد أوالمعلومات المتاحة أثناء تنفيذه يمكن أن ترسل بوسائل إلكترونية إذا وافق المرسل إليهم على إستخدام هذه الوسائل الإلكترونية. ومن المفترض أن يكون إستخدام الوسائل الإلكترونية أمر مقبول مالم يكن المتلقى قد صرح مسبقا بأنه يفضل وسائل أخرى للإتصال.

2. على مقدم الخدمة أو المورد الذي يعرض سلعاً وخدمات بشكل مهني وبوسائل إلكترونية، وضع الشروط التعاقدية المعمول بها بشكل مباشر أو غير مباشر وبما يسمح بالمحافظة وإستنساخ مثل هذه الشروطا وفقا للتشريعات الوطنية.

3. لإبرام العقد بشكل صحيح، يجب أن يكون الشخص المعروض عليه السلعة أو الخدمة قد أتيحت له إمكانية التحقق من صحة تفاصيل طلبه، خاصةً السعر قبل تأكيد الطلب المذكور والإعراب عن القبول به.

4. على الشخص الذي يعرض سلع وخدمات الإقرار بإستلام الطلب الموجه إليه دون تاخير غير مبرر وبوسائل إلكترونية.
يعد الطلب وتأكيد قبول العرض والإقرار بالإستلام مستوفاة عندما تكون الأطراف الموجهة إليها قد تمكنت من الحصول عليه.

5. يجوز إستثناء الإتفاقيات المبرمة بين الشركات والمهنيين (B2B) من أحكام المادتين 3.5 و 4.5 من هذه الإتفاقية.

6. أ) يكون أي شخص طبيعي أو معنوي يمارس النشاط المحدد في الفقرة الأولى من المادة. 1.2 من هذه الإتفاقية مسؤولاً بحكم طبيعة الحال إزاء الطرف المتعاقد الآخر عن الوفاء بالإلتزامات الناشئة عن العقد بغض النظر عما إذا كان يجب الوفاء بهذه الإلتزامات من قبله أو من قبل مزودين آخرين للخدمات، وذلك دون المساس بحقه في المطالبة ضد هؤلاء المزودين.

ب) ومع ذلك، يجوز للشخص الطبيعي أو المعنوي تبرأت نفسه من كل المسؤولية أو جزء منها عند إثبات أن عدم تنفيذ العقد أو سوء تنفيذه يعزى إلي شريكه أو إلى قوة قاهرة.

المادة

الكتابة في شكل إلكتروني

1. دون المساس بالأحكام التشريعية السارية في الدولة الطرف، لايجوز إجبار أي شخص على إتخاذ إجراء قانوني بوسائل إلكترونية.

أ) إذا دعت الحاجة إلى وثيقة مكتوبة للتحقق من صحة إجراء قانوني، تنشئ كل دولة طرف الشروط القانونية للتكافؤ الوظيفي بين الإتصالات الإلكترونية والوثائق الورقية، عندما يتطلب النظام الداخلي الساري وثيقة مكتوبة لإثبات صحة العمل القانوني؛

ب) إذا كانت الوثيقة الورقية خاضعة لشروط خاصة مثل الوضوح أو العرض، فيجب أن تخضع الوثيقة المكتوبة في شكل إلكتروني لنفس الشروط؛

ج) وتعتبر متطلبات إرسال عدة نسخ من وثيقة مكتوبة في شكل إلكتروني مستوفاة إذا كان في الإمكان إعادة إستنساخ الوثيقة في شكل مادي بواسطة المرسل إليه.

. 2 يستثنى التالي من أحكام المادة 2.6 من هذه الإتفاقية:

أ) الأعمال الخاصة التي يتم التوقيع عليها والتي تتعلق بقانوني الأسرة والميراث؛

ب) الأعمال ذات الطبيعة المدنية أو التجارية التي تتم بموجب توقيع خاص وتتعلق بالضمانات الشخصية أو الحقيقية وفقا للتشريعات المحلية، إلا إذا تمت هذه الأعمال على يد شخص لأغراض مهنته.

. 3 يتم إستلام الوثيقة المكتوبة في شكل إلكتروني عندما يحاط المرسل إليه علما علي النحو الواجب بذلك ويقر بإستلامها.

. 4 ونظرا للوظيفة الضريبية للفواتير، يجب أن تكون مكتوبة لضمان سهولة قراءتها، وسلامة وإستدامة مضمونها. ويجب ضمان صحة أصلها.

ومن بين الطرق التي يمكن تنفيذها لتحقيق الأهداف الضريبية للفواتير، وضمان أداء وظائفها، هو إقامة ضوابط إدارية تنجم عنها عملية مراجعة للحسابات موثوق بها بين الفاتورة والتزويد بالسلع أو بالخدمات.

بالإضافة إلى أنواع الضوابط المحددة في الفقرة 1، فإن الطرق التالية تعد أمثلة على التقنيات التي تضمن مصداقية أصل وسلامة المحتويات للفاتورة الإلكترونية.

(أ) التوقيع الألكتروني المؤهل على النحو المحدد في المادة 1؛

(ب) التبادل الإلكتروني للبيانات، الذي يفهم على أنه نقل إلكتروني من حاسوب إلى آخر، للبيانات التجارية والإدارية في شكل رسالة تبادل إلكترونى للبيانات وفقا لمعايير متفق عليها، شريطة أن ينص الإتفاق المتعلق بهذا التبادل على إستخدام إجراءات كفيلة بصحة أصل منشأ البيانات وسلامتها.

. 5 تكون الوثيقة المكتوبة في شكل إلكتروني مقبولة كدليل معادل للوثيقة الورقية ويكون لها نفس الحجية القانونية، شريطة أن يتسنى التعرف، علي النحو الواجب، على هوية الشخص الذي صدرت منه الوثيقة وأنه تم إعدادها وحفظها في ظروف تضمن سلامتها.

القسم 3 : تأمين المعاملات الإلكترونية

المادة7

ضمان تأمين المعاملات الإلكترونية

1. أ) يجب أن يسمح مزود السلع لعملائه أن ينفذوا مدفوعاتهم بإستخدام طرق دفع إلكترونية توافق عليها الدولة وفقا للأنظمة المعمول بها في كل دولة طرف.

ب) يتعين على مزود السلع أو مقدم الخدمات بوسائل إلكترونية والذي يدعي أداء إلتزام يجب أن يثبت وجود الألتزام أو يثبت أن الألتزام تم الوفاء به أو لم يكن موجودا.

2. إذا لم تنص الأحكام التشريعية للدول الأعضاء على مبادئ أخرى، وحيث لا توجد إتفاقية سارية بين الأطراف، يتولى القاضي تسوية نزاعات الإثبات من خلال استخدام كل الوسائل الممكنة لتحديد المطالبة الأكثر قبولا بغض النظر عن مصدر الرسالة المستخدمة.

3. أ) يكون للنسخة أو لأي إستنساخ آخر من العقود التي وقعت بالوسائل الإلكترونية له نفس القيمة الإثباتية للعقد ذاته، حيث قد تم إعتماد النسخة كصورة طبق الأصل من العقد المذكور بواسطة الهيئات المعتمدة حسب الأصول من قبل سلطة الدولة الطرف؛

ب) تؤدي عملية التصديق إلى إصدار، عند الضرورة، شهادة المطابقة.

4. أ) يكون التوقيع الإلكتروني الذي يتم إنشاءه بواسطة جهاز مؤمن، والذي يستطيع الموقع أن يبقيه تحت مراقبته الحصرية ويتم إلحاقه شهادة رقمية، مقبولاً بنفس الشروط المماثلة للتوقيع بخط اليد؛

ب) يفترض موثوقية الإجراء، مالم يثبت خلاف ذلك، عندما يتم إنشاء التوقيع الإلكتروني بواسطة جهاز إنشاء توقيع مؤمن، يضمن سلامة الفعل ويتم ضمان التعرف على هوية القائم بالتوقيع.

الفصل 2

حماية البيانات ذات الطابع الشخصي

القسم 1 : حماية البيانات ذات الطابع الشخصي

المادة 8

أهداف هذه الإتفاقية بخصوص البيانات ذات الطابع الشخصي

1- تلتزم كل دولة طرف بوضع إطار قانوني يهدف إلى تعزيز الحقوق الاساسية والحريات العامة، لا سيما حماية البيانات الفعلية، وقمع أية جريمة متعلقة بإنتهاك الخصوصية والمعاقبة عليها دون المساس بمبدأ حرية حركة البيانات ذات الطابع الشخصي.

2- يجب أن تضمن هذه الآلية المنشئة أن أي نوع من معالجة للبيانات يجب أن يحترم الحريات والحقوق الأساسية للأشخاص الطبيعيين مع الأخذ بعين الإعتبار صلاحيات الدولة وحقوق المجتمعات المحلية والأهداف التي أنشئت من أجلها المشاريع التجارية.

المادة 9 : مجال تطبيق الأتفاقية

1. يجب أن تكون الأجراءت التالية خاضعة لهذه الإتفاقية:

أ) أي جمع أو معالجة أو إرسال أو تخزين أو إستخدام للبيانات ذات الطابع الشخصي من قبل شخص طبيعي أو الدولة أو المجتمعات المحلية، والهيئات الإعتبارية العامة أو الخاصة؛

ب) أي معالجة آلية او غير آلية لبيانات واردة أو من المفترض أن تكون جزء من ملف، باستثناء أوجه المعالجة المذكورة في المادة 2.9 من هذه الاتفاقية؛

ج) أي معالجة للبيانات تتم في أراضي دولة عضو في الإتحاد الإفريقي؛

د) أي معالجة للبيانات تتصل بالأمن العام، الدفاع، البحث العلمي، الملاحقة الجنائية أو أمن الدولة، مع مراعاة الأستثناءات التي تحددها الأحكام المحددة في قوانين أخرى سارية.

2. لا تطبق هذه الاتفاقية على الآتي:

أ) معالجة البيانات التي يقوم بها شخص طبيعي ضمن الإطار الحصري لأنشطته الشخصية أو المنزلية، شريطة أن مثل هذه البيانات ليست بغرض الإتصال المنتظم بأطراف ثالثة أو لنشرها؛

ب) النسخ المؤقتة المستخرجة ضمن إطار الأنشطة الفنية للإرسال والوصول إلى شبكة رقمية بهدف تخزين آلي، وسيط، ومؤقت للبيانات ولغرض وحيد وهو تمكين منتفعين آخرين بخدمات الحصول على المعلومات المرسلة بشكل أفضل.

المادة 10

الإجراءات الأولية لمعالجة البيانات ذات الطابع الشخصي

1 . تستثنى الأفعال الآتية من الإجراءات الأولية:

أ) المعالجات المذكورة في المادة 2.9 من هذه الاتفاقية؛

ب) المعالجات التي تضطلع علي هدف وحيد هو حفظ سجل حصريا للإستعمال الشخصي؛

ج) المعالجات التي تنفذها جمعية أو أية هيئة غير ربحية ذات هدف ديني، فلسفي، سياسي، أو نقابي، شريطة أن تكون البيانات منسجمة مع أهداف الجمعية أو الهيئة المذكورة، وتتعلق فقط بأعضائها، وأن البيانات لم يكشف عنها لطرف ثالث.

2. بإستثناء الحالات المنصوص عليها في المادة 1.10 أعلاه وفي المادتين 4.10 و 5.10 من هذه الإتفاقية، معالجة البيانات ذات الطابع الشخصي يجب أن تخضع للإعلان لدي سلطة الحماية.

3. فيما يتعلق بالحالات الأكثر شيوعاً لمعالجة البيانات ذات الطابع الشخصي التي ليس من المرجح أن تشكل إنتهاكاً للحياة الخاصة أو للحريات الفردية، يجوز لسلطة الحماية وضع ونشر معايير بهدف تبسيط الإلتزام بالإعلان أو الإعفاء منه.

4. يجب أن تتخذ الإجراءات التالية بعد الحصول على إذن من السلطة الوطنية للحماية:

أ) معالجة بيانات ذات طابع شخصي ومتعلقة بمعلومات وراثية وبحوث في المجال الصحي؛

ب) معالجة بيانات ذات طابع شخصي ومتعلقة بمعلومات حول الجرائم أو الإدانات الجنائية أو التدابير الأمنية؛

ج) معالجة بيانات ذات طابع شخصي بغرض ربط ملفات كما هو منصوص في المادة 15 من هذه الاتفاقية أو معالجة بيانات متعلقة برقم هوية وطني أو أية هوية أخرى ذات طبيعة مشابهة؛

د) معالجة بيانات ذات طابع شخصي تشمل بيانات المقاييس الحيوية؛

هـ) معالجة بيانات ذات طابع شخصي تتعلق بالمصلحة العامة، لا سيما لأغراض تاريخية أو إحصائية أو علمية.

5. معالجة البيانات ذات الطابع الشخصي التي تتم بالنيابة عن الحكومة، والمؤسسات العامة، والمجتمع المحلي، وهيئة اعتبارية من القطاع الخاص تعمل في الخدمة العامة، يجب أن يكون وفقا لقانون تشريعي أو تنظيمي يصدر بعد المشورة المستنيرة لسلطة الحماية. تترتبط معالجة هذة البيانات بما يلي:

أ) أمن الدولة والدفاع أو الأمن العام؛

ب) الوقاية والتحقيق والكشف أو الملاحقة القضائية للجرائم الجنائية، أو تنفيذ إدانات جنائية أو تدابير أمنية؛

ج) المسح المكاني؛

د) البيانات ذات طابع شخصي التي تكشف بطريقة مباشرة أو غير مباشرة عن الأصل العرقي أو الإثني أو الإقليمي، أو الإنتماء، أو المعتقدات السياسية أو الفلسفية أو الدينية أو الإنتماء النقابي للأشخاص أو بيانات متعلقة بالصحة أو بالحياة الجنسية.

6. يجب أن توضح طلبات الرأي والإعلانات وطلبات الترخيص ما يلي:

أ) هوية وعنوان الموظف الذي يعالج البيانات، أو هوية وعنوان ممثله المفوض بحسب الأصول، في حالة عدم إستقراره في أراضي الدولة الطرف في الإتحاد الإفريقي؛

ب) هدف (أهداف) المعالجة ووصف عام لمهامها؛

ج) الترابط المتوخي أو سائر أشكال التنسيق مع أنشطة المعالجة الأخرى؛

د) البيانات ذات الطابع الشخصي المعالجة، وأصلها وفئات الأشخاص المشاركين في المعالجة؛

هـ) مدة الاحتفاظ بالبيانات المعالجة؛

و) الخدمة أو الخدمات المسؤولة عن إجراء عملية المعالجة بالإضافة إلى فئة الأشخاص المتطلعين على البيانات المسجلة بحكم وظائفهم أو مقتضيات الخدمة؛

ز) الأشخاص المصرح لهم بتلقي الإتصالات المتعلقة بالبيانات؛

ح) وظيفة الشخص أو نوع الخدمة التي يمارس فيها حق الإطلاع على البيانات؛

ط) التدابير المتخذة لضمان أمن إجراءت المعالجة والبيانات؛

ي) الإشارة إلى إستخدام مقاول فرعي؛

ك) النقل المتوقع للبيانات ذات الطابع الشخصي إلى بلد ثالث ليس عضواً في الإتحاد الإفريقي، شريطة المعاملة بالمثل.

7. سوف تتخذ سلطة الحماية الوطنية قرارا خلال فترة زمنية محددة إعتبارا من تاريخ إستلام طلب الرأي أو الترخيص. غير أنه، من الجائز تمديد أو عدم تمديد هذه الفترة الزمنية بناء على قرار مدروس تتخذه سلطة الحماية الوطنية .

8. الإخطار والإعلان أو طلب الترخيص تكون موجهة إلى سلطة الحماية الوطنية بالوسائل الإلكترونية أو عن طريق البريد.

9. يجوز الإتصال بسلطة الحماية الوطنية من قبل أي شخص من تلقاء نفسه أو بواسطة محام أو أي شخص طبيعي أو قانوني آخر مكلف، حسب الأصول.

القسم 2 : الإطار المؤسسي لحماية البيانات ذات الطابع الشخصي

المادة 11

وضع، تشكيل وتنظيم سلطات الحماية الوطنية للبيانات ذات الطابع الشخصي

1. أ) تلتزم كل دولة طرف بإنشاء سلطة مسؤولة عن حماية البيانات ذات الطابع الشخصي؛

ب) تكون لسلطة الحماية الوطنية سلطة إدارية مستقلة وهي مكلفة بضمان معالجة البيانات ذات الطابع الشخصي وفقا لأحكام هذه الإتفاقية.

2. تقوم سلطة الحماية الوطنية بإطلاع الأشخاص المعنيين والمسؤولين عن معالجة البيانات بحقوقهم وواجباتهم.

3. دون المساس بالمادة 6.11 ، تحدد كل دولة طرف تكوين السلطة الوطنية المكلفة بحماية البيانات ذات الطابع الشخصي.

4. يجوز دعوة المسؤولين المحلفين باليمين الدستورية المشاركة في بعثات التدقيق وفقا لأحكام موجودة في الدول الأطراف.

5. أ) يخضع أعضاء سلطة الحماية الوطنية للسرية المهنية وفقا للنصوص السارية في كل دولة طرف؛

ب) يجب على كل سلطة حماية وطنية صياغة قواعد إجراءية والتي تتضمن، في جملة أمور، القواعد التي تحكم مداولات ومعالجة وعرض الحالات.

6. العضوية في سلطة الحماية الوطنية غير متوافقة مع العضوية في الحكومة، ومع تنفيذ مهام رجال الأعمال ومالكي الأسهم في الشركات الخاصة بقطاع تكنولوجيا المعلومات والإتصالات.

7. أ) دون المساس بالتشريعات الوطنية، يتمتع أعضاء سلطة الحماية الوطنية بالحصانة الكاملة فيما يخص الآراء التي يعبرون عنها عند ممارستهم لمهامهم أو أي شي يتعلق بالسعي لتحقيقها؛

ب) لا يتلقى أعضاء سلطة الحماية الوطنية تعليمات من أي جهة عند ممارستهم لمهامهم.

8. تلتزم الدول الأطراف بتزويد سلطة الحماية الوطنية بالموارد البشرية والفنية والمالية اللازمة لإنجاز مهامها.

المادة 12

واجبات وصلاحيات سلطات الحماية الوطنية

1. سلطة الحماية الوطنية مكلفة بأن تعمل علي ضمان أن معالجة البيانات ذات الطابع الشخصي تتم وفقا لأحكام هذه الإتفاقية في الدول الأطراف في الإتحاد الإفريقي.

2. يجب أن تضمن سلطات الحماية الوطنية أن تكنولوجيا المعلومات والإتصالات لاتشكل تهديداً للحريات العامة للمواطنين وحياتهم الخاصة. ولهذه الغاية، فهى مكلفة بما يلي:

أ) الإستجابة لكل طلب للرأي متعلق بمعالجة البيانات ذات الطابع الشخصي؛

ب) إعلام الأشخاص المعنيين والمسؤولين عن عملية معالجة البيانات بحقوقهم وواجباتهم؛

ج) السماح، في عدد من الحالات، بمعالجة ملفات البيانات، لا سيما الملفات الحساسة؛

د) تلقي الإجراءات الأولية لمعالجة البيانات ذات الطابع الشخصي؛

هـ) تلقي الدعاوى والعرائض والشكاوى المتعلقة بمعالجة البيانات ذات الطابع الشخصي وإعلام أصحابها بالنتائج المتعلقة بها؛

و) علي وجه السرعة، إبلاغ السلطة القضائية بأنواع معينة من المخالفات والإنتهاكات التي علمت بها؛

ز) إجراء مراجعة لكافة البيانات ذات الطابع الشخصي المعالجة، وذلك بواسطة موظفيها أو المسؤولون المحلفون بالقسم؛

ح) فرض عقوبات إدارية ومالية على مسؤولي معالجة البيانات؛

ط) تحديث الدليل الذي هو في متناول الجمهور بالبيانات ذات الطابع الشخصي التي تمت معالجتها؛

ي) تقديم المشورة للأشخاص والهيئات العاملة في مجال معالجة البيانات الشخصية أو في إجراء الإختبارات والتجارب التي من المرجح أن تؤدي إلى معالجة للبيانات؛

ك) التفويض بنقل البيانات ذات الطابع الشخصي عبر الحدود؛

ل) تقديم مقترحات كفيلة بتبسيط وتحسين الأطر التشريعية والتنظيمية لمعالجة البيانات؛

م) إنشاء آليات للتعاون مع سلطات حماية البيانات ذات الطابع الشخصي لدول ثالثة؛

ن) المشاركة في مفاوضات دولية بشأن حماية البيانات ذات الطابع الشخصي؛

س) إعداد تقرير للفعاليات وفقا لدورية واضحة لكي يتم تقديمه إلى الجهات المختصة في الدولة الطرف.

3. يجوز لسلطات الحماية الوطنية إتخاذ التدابير التالية:

أ) توجيه إنذار لأي موظف مسؤول عن معالجة البيانات لا يتقيد بالإلتزامات الناجمة عن هذه الإتفاقية؛

ب) إرسال خطاب تحذير رسمي لوقف هذه الإنتهاكات في إطار زمني محدد من قبل السلطة.

4. يجوز لسلطات الحماية الوطنية، في حال عدم إمتثال الشخص المسؤول عن معالجة البيانات للخطاب التحذيري الرسمي الموجه إليه، أن تفرض، بعد إجراءات الطعن، العقوبات التالية:

أ) سحب مؤقت للرخصة الممنوحة؛

ب) سحب دائم للرخصة؛

ج) فرض غرامة مالية.

5. في حالات الطوارئ، حيث تؤدي معالجة أو إستخدام البيانات ذات الطابع الشخصي إلى إنتهاك الحقوق والحريات الأساسية، يجوز لسلطات الحماية الوطنية (بعد إجراءات الطعن) تقرير ما يلي:

أ) إيقاف معالجة البيانات؛

ب) حجب بعض البيانات المعالجة ذات الطابع الشخصي؛

ج) حظر مؤقت أو دائم لأي معالجة مخالفة لأحكام هذه الإتفاقية.

6. تخضع العقوبات المفروضة والقرارات المتخذة من قبل سلطات الحماية الوطنية للإستئناف.

القسم 3: االإلتزامات المتعلقة بالشروط التي تحكم معالجة البيانات ذات الطابع الشخصي

المادة 13

المبادئ الأساسية التي تحكم معالجة البيانات ذات الطابع الشخصي

المبدأ 1: مبدأ الموافقة والشرعية في معالجة البيانات ذات الطابع الشخصي

تعتبر معالجة البيانات ذات الطابع الشخصي مشروعة إذا وافق عليها الشخص المعني. شرط الموافقة هذا يمكن التنازل عنه إذا كانت المعالجة ضرورية للآتي:

أ) الإمتثال لإلتزام قانوني يخضع له المسؤول عن عملية المعالجة؛

ب) لتنفيذ مهمة ذات مصلحة عامة أو في ممارسة السلطة الرسمية المخولة للمسؤول عن المعالجة أو لطرف ثالث تم الإفصاح له بالبيانات؛

ج) لتنفيذ عقد يعتبر الشخص موضوع البيانات طرفا فيه أو لإتخاذ إجراءات تعاقدية بناء على طلبه قبل الشروع في التعاقد؛

د) لحماية المصالح الحيوية أو الحقوق والحريات الأساسية للشخص موضوع البيانات.

المبدأ 2: مبدأ القانونية والنزاهة في معالجة البيانات ذات الطابع الشخصي

يجب أن يتم جمع وتسجيل ومعالجة وتخزين ونقل البيانات ذات الطابع الشخصي بطريقة قانونية ونزيهة وخالية من الإحتيال.

المبدأ 3: مبدأ القصد، الصلة والتخزين للبيانات ذات الطابع الشخصي المعالجة

أ) يجب أن يكون جمع البيانات من أجل أهداف محددة، واضحة وشرعية، ولا يجوز معالجة تلك البيانات لاحقا بما يتعارض مع الأهداف المذكورة؛

ب) يجب أن تكون البيانات كافية وذات صلة وغير مفرطة فيما يتعلق بالأهداف التي من أجلها تم جمع البيانات ومن ثم القيام بمعالجتها؛

ج) يجب حفظ البيانات لمدة لا تتجاوز المدة المطلوبة لتحقيق الأهداف التي تم من أجلها تم جمع البيانات ومن ثم القيام بمعالجتها؛

د) لايجوز بعد الفترة المذكورة الإحتفاظ بالبيانات إلا لتلبية إحتياجات محددة لمعالجة البيانات لأغراض تاريخية أو إحصائية أو بحوثية وذلك وفقا للأحكام القانونية.

المبدأ 4: مبدأ الدقة في البيانات ذات الطابع الشخصي

البيانات التي تم جمعها يجب أن تكون دقيقة، وعند الضرورة حديثة. يجب إتخاذ كل الخطوات المعقولة لضمان أن البيانات التي هي غير دقيقة أو غير كاملة، مع مراعاة الأغراض التي جمعت من أجلها أو الأغراض التي بموجبها تمت معالجتها، يتم مسحها أو تصحيحها.

المبدأ 5: مبدأ الشفافية في معالجة البيانات ذات الطابع الشخصي

يتطلب مبدأ الشفافية الكشف الإلزامي عن المعلومات فيما يتعلق بالبيانات ذات الطابع الشخصي من جانب المسؤول عن عملية المعالجة.

المبدأ 6: مبدأ السرية والتأمين في معالجة البيانات ذات الطابع الشخصي

أ) يجب معالجة البيانات ذات الطابع الشخصي بشكل سري مع توفير الحماية، لا سيما عندما تشمل المعالجة نقل البيانات على شبكة إتصال؛

ب) عندما يتم تنفيذ المعالجة لحساب المسؤول عن عملية المعالجة، يتعين عليه إختيار معالج تتوفر لديه ضمانات كافية. ويكون لزاما على هذا المسؤول وعلى المعالج الإلتزام بالإجراءات الأمنية المنصوص عليها في هذه الإتفاقية.

المادة 14

المبادئ المحددة المتعلقة بمعالجة البيانات الحساسة

1. تتعهد الدول الأطراف بحظر أي جمع للبيانات ومعالجتها تكشف الأصل العرقي والإثني والإقليمي، أو البنوة الأبوية أو الآراء السياسية أو المعتقدات الدينية أو الفلسفية أو الإنتماء النقابي، الحياة الجنسية والمعلومات الوراثية أو، بشكل عام، بيانات عن الحالة الصحية للشخص المعني.
2. لا يسري الحظر المنصوص عليه في المادة 1.14 علي الفئات التالية، حيث:

أ) تشمل المعالجة لبيانات منشورة بصورة عامة من قبل الشخص المعني؛

ب) أعطى الشخص المعني موافقته الخطية، أيا كانت الوسيلة، على المعالجة ووفقا للنصوص السارية؛

ج) تكون معالجة البيانات ذات الطابع الشخصي ضرورية لحماية المصالح الحيوية للشخص المعني أو لشخص آخر في حالة عجز الشخص المعني جسدياً أو قانونياً عن إعطاء هذه الموافقة؛

د) تكون معالجة البيانات الجينية على وجه الخصوص ضرورية لأغراض الإثبات، وممارسة أو الدفاع عن المطالبات القانونية؛

هـ) عند إقامة إجراء قضائي أو التحقيق الجنائي؛

و) تكون معالجة البيانات ذات الطابع الشخصي ضرورية للمصلحة العامة، خاصة لأغراض تاريخية أو إحصائية أو علمية؛

ز) لتنفيذ عقد يعتبر الشخص موضوع البيانات طرفا فيه أو لإتخاذ إجراءات تعاقدية بناء علي طلبه قبل الشروع في التعاقد؛

ح) عندما تكون المعالجة ضرورية للإمتثال لإلتزام قانوني أو تنظيمي يخضع له الشخص المسؤول عن المعالجة؛

ط) تكون المعالجة ضرورية لتنفيذ مهمة ذات منفعة عامة أو مهمة تقوم بها السلطة الرسمية أو تسندها هذه السلطة المخولة إلى المسؤول عن المعالجة أو إلى طرف ثالث تم الإفصاح له عن البيانات؛

ي) عندما تتم المعالجة في إطار الأنشطة المشروعة لمؤسسة أو جمعية أو أي كيان آخر غير ربحي لأغراض سياسية أو فلسفية أو دينية أو تعاونية أو لأغراض نقابية، وبشريطة أن تتعلق المعالجة فقط بأعضاء الكيان المذكور أو الأشخاص الذين يقومون بإتصالات منتظمة معه مرتبطة بتحقيق أهدافه، شريطة عدم نقل البيانات لطرف ثالث دون موافقة الأشخاص المعنيين.

3. تكون معالجة البيانات ذات الطابع الشخصي لأغراض صحفية أو لغرض الأبحاث أو لأغراض فنية أو للتعبير الأدبي، مقبولة حيث يكون الهدف من المعالجة حصرياً للتعبير الأدبي والفني أو للممارسة المهنية لنشاط صحفي أو بحثي وفقا لقواعد أخلاقيات هذه المهن.

4. تطبيق أحكام هذه الإتفاقية يجب أن لا يحول دون تطبيق التشريعات الوطنية فيما يتعلق بوسائل الإعلام المطبوعة أو المسموعة أو المرئية فضلا علي أحكام القانون الجنائي التي تنص علي شروط ممارسة حق الرد، والتي تمنع، وتحد، وتعوض علي، وعند الضرورة، قمع إنتهاكات الخصوصية والأضرار التي لحقت بسمعة الفرد.

5. يجب أن لا يكون الشخص رهنا بقرار تنتج عنه آثار قانونية متعلقة به أو تؤثر عليه إلى درجة كبيرة، وهذه النتائج والآثار إنما كانت تستند فقط على المعالجة الآلية للبيانات التي كان القصد منها تقييم بعض الجوانب الشخصية المتعلقة به.

6. أ) لايجوز للمسؤول عن معالجة البيانات نقل بيانات ذات طابع شخصي إلى دولة ليست عضواً في الإتحاد الأفريقي ما لم تضمن هذه الدولة مستوى كافيا من حماية الحياة الخاصة والحريات والحقوق الأساسية للأشخاص الذين تخضع بياناتهم للمعالجة أو من من المحتمل أن تتم معالجتها؛

ب) لا ينطبق الحظر الوارد أعلاه، في حالة عندما يتقدم مسؤول معالجة البيانات بطلب إذنا بهذا النقل من سلطة الحماية الوطنية قبل ان يتم نقل أي بيانات ذات طابع شخصي إلى البلد الثالث.

المادة 15

ترابط ملفات البيانات ذات الطابع الشخصي

يجب أن يمكن ترابط الملفات الموضح في المادة 4.10 من هذه الاتفاقية من تحقيق أهداف قانونية وتشريعية تمثل مصلحة مشروعة لموظفي معالجة البيانات. ويجب أن تخضع لتدابير أمنية مناسبة، وأيضا أن تأخذ في الإعتبار مبدأ الصلة للبيانات التي سيتم ترابطها.

القسم 4: حقوق الشخص موضوع البيانات ذات الطابع الشخصي

المادة 16

الحق في المعلومات

على المسؤول عن معالجة البيانات تزويد الشخص الذي ستعالج بياناته، في موعدٍ لا يتجاوز الوقت الذي يتم فيه جمع هذه البيانات، بغض النظر عن الوسائل والتسهيلات المستخدمة، بالمعلومات التالية:

أ) هويته، وإن وجدت، هوية ممثله؛

ب) أغراض المعالجة التي تستهدفها البيانات؛

ج) فئات البيانات المعنية؛

د) المتلقي (المتلقون) الذي (الذين) قد يتم له (لهم) الكشف عن البيانات؛

هـ) القدرة علي طلب الشطب من الملف؛

و) وجود الحق في الإطلاع على البيانات الخاصة بالشخص والحق في تصحيحها؛

ز) مدة الإحتفاظ بالبيانات؛

ح) إقتراح نقل البيانات إلى بلدان ثالثة.

المادة 17

الحق في الوصول الى المعلومات

يحق لأي شخص طبيعي ستعالج بياناته الشخصية الطلب من الموظف القائم بهذه المعالجة تزويده، في شكل أسئلة، بما يلي:

أ) المعلومات التي من شأنها تمكينه من تقييم والإعتراض علي المعالجة؛

ب) تأكيد معالجة أو عدم معالجة البيانات الخاصة به؛

ج) نقل للشخص البيانات ذات الطابع الشخصي التي تحت المعالجة بالإضافة إلى أي معلومات أخرى متوفرة عن مصدر هذه البيانات؛

د) معلومات عن الغرض من المعالجة، فئات البيانات الشخصية المعنية، والمستفيدين أو فئات المتلقين الذين تم الإفصاح لهم عن البيانات.

المادة 18

الحق في الإعتراض

من حق أي شخص طبيعي الإعتراض، لأسباب مشروعة، على معالجة البيانات ذات الطابع الشخصي الخاصة به.

وله الحق في إبلاغه قبل كشف بياناته، للمرة الأولى، إلى طرف ثالث أو إستخدامها بالنيابة عن طرف ثالث لإغراض التسويق، وأن يعرض عليه صراحةً حق الإعتراض، مجانا، على هذه الإفصاحات أو الإستخدامات.

المادة 19

حق التصحيح أو الحذف

يجوز لأي شخص طبيعي الطلب من مسؤول معالجة البيانات تصحيح أو إكمال أو تحديث أو حجب أو حذف، حسب الإقتضاء، للبيانات ذات الطابع الشخصي الخاصة به في حال إن كانت هذه البيانات خاطئة أو ناقصة أو غير واضحة أو قديمة، أو تم حظر جمعها أو إستعمالها أو كشفها أو الإحتفاظ بها.

القسم 5: إلتزامات المسؤول عن معالجة البيانات ذات الطابع الشخصي

المادة 20

إلتزامات السرية

يجب أن تكون معالجة البيانات ذات الطابع الشخصي سرية. ويجب أن تتم المعالجة حصرياً بواسطة أشخاص يعملون تحت سلطة المسؤول عن معالجة البيانات وبموجب تعليمات صادرة منه.

المادة 21

إلتزامات التأمين

يتعين على مسؤول المعالجة إتخاذ جميع الإحتياطات اللازمة، بناءً على طبيعة البيانات، لا سيما، منع تغيير هذه البيانات أو إتلافها أو الإطلاع عليها من قبل أطراف ثالثة غير مرخص لها بذلك .

المادة 22

إلتزامات التخزين

يجب حفظ البيانات ذات الطابع الشخصي لمدة لا تتجاوز المدة الضرورية لتحقيق الهدف من جمع ومعالجة البيانات المذكورة.

المادة 23

إلتزامات الإستدامة

أ) على المسؤول عن المعالجة إتخاذ كافة التدابير المناسبة لضمان أن البيانات ذات الطابع الشخصي المعالجة يمكن إستخدامها، بغض النظر عن الجهاز التقني المستخدم في العملية؛

ب) على مسؤول المعالجة أن يضمن، على وجه الخصوص، أن لا تشكل التطورات التقنية عائقاً أمام هذا الإستعمال.

الفصل 3

تعزيز الأمن الإلكتروني ومكافحة الجريمة الإلكترونية

القسم 1: تدابير الأمن الإلكتروني الواجب إتخاذها على المستوى الوطني

المادة 24

إطار تأمين الفضاء الإلكتروني الوطني

1. السياسة الوطنية

تلتزم كل دولة طرف – بالتعاون مع أصحاب المصلحة – بوضع سياسة وطنية لأمن الفضاء الإلكتروني والتي تعترف بأهمية البنية التحتية الأساسية للمعلومات بالنسبة للدولة، وتحدد المخاطر التي تواجهها بإستخدام نهج لمكافحة كافة المخاطر وتوضح طريقة تنفيذ أهداف هذه السياسة.

2. الإستراتيجية الوطنية

يجب علي كل الدول الاطراف إعتماد إستراتيجيات فيما تراه مناسبا وكافيا لتنفيذ سياسة وطنية للأمن الفضائي الإلكتروني، لاسيما في مجال الإصلاح التشريعي والتنمية ورفع مستوى التوعية وبناء القدرات، والشراكة بين القطاعين العام والخاص، والتعاون الدولي، على سبيل المثال لا الحصر. وتحدد هذه الإستراتيجيات الهياكل التنظيمية والأهداف والأطر الزمنية لتنفيذ سياسة الأمن الفضائي الإلكتروني بنجاح من خلال وضع الأساس للإدارة الفعالة لحوادث أمن الفضاء الإلكتروني والتعاون الدولي.

المادة 25

التدابير القانونية

1. تشريعات مكافحة جريمة الفضاء الإلكتروني

تلتزم كل دولة طرف بإعتماد تدابير تشريعية و/أو تنظيمية تراها فعالة لتجريم كافة الأعمال الجنائية التي تؤثر على سرية ونزاهة وتوافر وبقاء أنظمة تكنولوجيا المعلومات والإتصالات، والبيانات التي تعالجها والبنية التحتية للشبكات الأساسية، فضلا عن إتخاذ تدابير إجرائية فعالة لمتابعة وملاحقة المخالفين. تأخذ الدول الأطراف بعين الإعتبار إختيار اللغة المستخدمة في أفضل الممارسات الدولية.

2. السلطات التنظيمية الوطنية

تلتزم كل دولة طرف بإعتماد تدابير تشريعية و/ أو تنظيمية تراها ضرورية لإسناد مسؤولية محددة إلى المؤسسات، سواء المنشأة حديثا او القائمة سابقا، وكذلك الموظفين المعينين لهذه المؤسسات المذكورة بغية منحهم سلطة وأهلية قانونية للتصرف في جميع جوانب تطبيق الأمن الفضائي

الإلكتروني، بما يشمل، على سبيل المثال لا الحصر، الإستجابة لحوادث أمن الفضاء الإلكتروني والتنسيق والتعاون في مجال العدالة التصالحية، تحقيقات الطب الشرعي والنيابة العامة، الخ..

3. حقوق المواطنين

عند إعتماد تدابير قانونية في مجال الأمن الفضائي الإلكتروني ووضع أطر لتنفيذها، تحرص كل دولة طرف أن لا تعيق هذه الإجراءات المعتمدة حقوق المواطنين التي يضمها الدستور الوطني والقوانين الداخلية، والحقوق التي تحميها الإتفاقيات الدولية، لاسيما الميثاق الأفريقي لحقوق الإنسان والشعوب، وكذلك الحقوق الأساسية مثل الحق في حرية التعبير وإحترام الخصوصية والحق في محاكمة عادلة، من بين إمور أخرى.

4. حماية البنية التحتية الحيوية

تلتزم كل دولة طرف بإعتماد إجراءات تشريعية و/ أو تنظيمية تراها ضرورية لتحديد القطاعات الحساسة لأمنها الوطني وإزدهار إقتصادها بالإضافة إلى أنظمة تكنولوجيا المعلومات والإتصالات المصممة للعمل في هذه القطاعات الحساسة بإعتبارها تشكل بنية تحتية حيوية للمعلومات؛ مع القيام في هذا الخصوص بإقتراح فرض عقوبات أكثر صرامة على الأعمال الإجرامية ضد أنظمة تكنولوجيا المعلومات والإتصالات في هذه القطاعات، وإتخاذ إجراءات وتدابير لتحسين اليقظة والتأمين والإدارة.

المادة 26

النظام الوطني لتأمين الفضاء الإلكتروني

1. ثقافة تأمين الفضاء الإلكتروني

أ) تلتزم كل دولة طرف بتشجيع ثقافة أمن الفضاء الإلكتروني بين جميع أصحاب المصلحة، أي، الحكومات والشركات والمجتمع المدني، والتي تطور وتملك وتدير وتشغل وتستخدم نظم

المعلومات والشبكات. ويجب أن تركز ثقافة أمن الفضاء الإلكتروني على الأمن عند القيام بتطوير أنظمة وشبكات للمعلومات، وإعتماد طرق جديدة للتفكير والتصرف عند إستخدام أنظمة المعلومات وكذلك خلال الإتصال أو المعاملات عبر الشبكات؛

ب) في إطار الترويج لثقافة أمن الفضاء الإلكتروني، يجوز أن تعتمد الدول الأطراف الإجراءات التالية: إنشاء خطة تأمين فضاء إلكتروني للأنظمة التي تديرها حكومات هذه الدول؛ إعداد وتنفيذ برامج ومبادرات للتوعية بالأمن لمستخدمي الأنظمة والشبكات؛ التشجيع على تطوير ثقافة أمن الفضاء الإلكتروني في المؤسسات؛ تعزيز مشاركة المجتمع المدني؛ وإطلاق برنامج مفصل وكامل للتوعية الوطنية لمستخدمي الإنترنت والشركات الصغيرة والمدارس والأطفال.

2. دور الحكومات

تلتزم كل دولة طرف بضمان لعب دور قيادي في تطوير ثقافة أمن الفضاء الإلكتروني داخل حدودها. وتلتزم الدول الأعضاء بالتوعية وتوفير التعليم والتدريب ونشر المعلومات للجمهور.

3. الشراكة بين القطاعين العام والخاص

تلتزم كل دولة عضو بتطوير الشراكة بين القطاعين العام والخاص كنموذج لإشراك الصناعة والمجتمع المدني والمجتمع الأكاديمي في ترويج وتعزيز أمن الفضاء الإلكتروني.

4. التعليم والتدريب

تلتزم كل دولة طرف بإتخاذ التدابير اللازمة لبناء القدرات بهدف توفير التدريب الذي يغطي جميع مجالات أمن الفضاء الإلكتروني لمختلف أصحاب المصلحة ووضع المعايير للقطاع الخاص.

تلتزم الدول الأطراف بتشجيع التعليم الفني للمهنيين العاملين في مجال تكنولوجيا المعلومات والاتصالات داخل وخارج الهيئات الحكومية من خلال إصدار الشهادات وتوحيد معايير التدريب؛ وتصنيف المؤهلات المهنية فضلا عن تطوير وتوزيع المواد التعليمية على أساس الإحتياجات.

المادة 27

الهياكل الوطنية لرصد تأمين الفضاء الإلكتروني

1. حوكمة أمن الفضاء الإلكتروني

أ) تقوم كل دولة طرف باتخاذ الإجراءات الكفيلة لإنشاء آلية مؤسسية ملائمة مسؤولة عن حوكمة أمن الفضاء الإلكتروني.

ب) **ويجب** ان تؤدي التدابير المتخذة وفقا للفقرة 1 من هذه المادة إلى إنشاء قيادة قوية، والإلتزام في جميع جوانب أمن الفضاء الإلكتروني للمؤسسات والمجموعات المهنية المعنية في كل دولة طرف. وفي هذا الصدد، تلتزم الدول الأطراف باتخاذ التدابير اللازمة من أجل:

1- تحديد المسؤولية الواضحة في مجال أمن الفضاء الإلكتروني على جميع مستويات الحكومة من خلال تحديد الأدوار والمسؤوليات بشروط محددة.

2- الإعراب عن إلتزام واضح وعلني وشفاف تجاه أمن الفضاء الإلكتروني.

3- تشجيع القطاع الخاص مع إلتماس إلتزامه ومشاركاته في المبادرات التي تقودها الحكومة من اجل تعزيز أمن الفضاء الإلكتروني.

ج) يجب أن تكون حوكمة أمن الفضاء الإلكتروني قائمة علي إطار وطني قادر على مواجهة التحديات ومعالجة جميع القضايا المتعلقة بأمن المعلومات على المستوى الوطني وفي أكبر عدد ممكن من مجالات أمن الفضاء الإلكتروني .

2. الإطار المؤسسي

تقوم كل دولة طرف بإعتماد التدابير التي تراها ضرورية لإنشاء المؤسسات المناسبة لمكافحة الجريمة الإلكترونية، ضمان الرصد والإستجابة للحوادث والتنبيهات، وضمان التنسيق الوطني وعبر الحدود من مشاكل أمن الفضاء الإلكتروني، وكذلك التعاون الدولي.

المادة 28

التعاون الدولي

1 . المواءمة

تلتزم الدول الاطراف بضمان أن التدابير التشريعية و/أو التنظيمية المعتمدة لمكافحة الجريمة الإلكترونية سوف تعزز إمكانية المواءمة الإقليمية لهذه التدابير وتحترم مبدأ المسؤلية الجنائية المزدوجة.

2. المساعدة القانونية المتبادلة

تلتزم الدول الأطراف التي ليس لديها إتفاقيات المساعدة المتبادلة في مجال الجريمة الإلكترونية، بالتشجيع على توقيع إتفاقيات المساعدة القانونية المتبادلة وفقا لمبدأ المسؤلية الجنائية المزدوجة مع القيام في الوقت نفسه بتعزيز تبادل المعلومات، فضلا عن تبادل البيانات على نحو فعال بين مؤسسات الدول الأطراف على أساس ثنائي ومتعدد الأطراف.

3. تبادل المعلومات

تلتزم الدول الأطراف بتشجيع إنشاء مؤسسات لتبادل المعلومات بشأن تهديدات الفضاء الإلكتروني وتقييم قابلية التعرض للخطر، مثل فرق الإستجابة لطوارئ الكمبيوتر، أو فرق الإستجابة لحوادث أمن الحاسوب.

4. وسائل التعاون

تلتزم الدول الأطراف بالإستفادة من وسائل التعاون الدولي القائمة بهدف الإستجابة للتهديدات الإلكترونية، وتحسين أمن الفضاء الإلكتروني وتشجيع الحوار بين أصحاب المصلحة. وربما قد تكون هذه الوسائل دولية، أو بين الحكومات، أو إقليمية، أو على أساس شراكات بين القطاعين العام والخاص.

القسم 2 : الأحكام الجنائية

المادة29

الجرائم الخاصة بتكنولوجيا المعلومات والإتصالات

1. الهجمات على أنظمة الكمبيوتر

تلتزم الدول الأطراف بإتخاذ التدابير التشريعية و/أو التنظيمية اللازمة لجعل الأفعال التالية جرائم جنائية:

أ) وصول أو محاولة للوصول الغير المصرح به إلى جزء أو كل نظام الحاسوب أو تجاوز الوصول المسموح به؛

ب) وصول أو محاولة للوصول الغير المصرح به إلى جزء أو كل نظام الحاسوب أو تجاوز الوصول المسموح به بقصد إرتكاب جريمة أخرى أو تسهيل إرتكاب مثل هذه الجريمة؛

ج) البقاء او محاولة البقاء عن طريق الإحتيال في كل أو جزء من نظام الحاسوب؛

د) إعاقة وتشويه أو محاولة لإعاقة أو تشويه أداء نظام الحاسوب؛

هـ) إدخال أو محاولة إدخال البيانات عن طريق الإحتيال في نظام الحاسوب؛

و) إتلاف أو محاولة إتلاف أو حذف أو محاولة حذف، أو إفساد او محاولة إفساد أو تغيير أو محاولة تغيير أو تعديل أو محاولة تعديل لبيانات الكمبيوتر عن طريق الإحتيال؛

وتلتزم الدول **الأطراف** كذلك بما يلي:

ز) أن تتبنى لوائح ونظم تلزم بائعي منتجات تكنولوجيا المعلومات والإتصالات بتقييم، من قبل خبراء وباحثين مستقلين، قابلية التأثر وضمان السلامة لمنتجاتهم وإطلاع المستهلكين على كل مواطن الضعف المكتشفة في المنتجات وكذلك الحلول الموصى بها لمعالجة مواطن الضعف المذكورة؛

ح) إتخاذ ما يلزم من إجراءات تشريعية أو تنظيمية لتجريم إنتاج بصورة غير قانونية، وبيع وإستيراد وحيازة أو نشر أو عرض أو التنازل أو تقديم المعدات المتاحة للكومبيوتر، أو برنامج، أو أي جهاز أو بيانات مصممة خصيصاً أو تكييفها لإرتكاب الجرائم، أو بصورة غير مشروعة توليد أو إنتاج كلمة السر، أو رمز وصول مماثل للبيانات الإلكترونية مما يتيح الوصول إلى جزء أو كل نظام الكمبيوتر.

2. الخروقات على البيانات المحوسبة

تلتزم الدول الأطراف بإتخاذ التدابير التشريعية و/أو التنظيمية اللازمة لجعل الأفعال التالية جرائم جنائية:

أ) إعتراض أو محاولة لإعتراض البيانات المحوسبة عن طريق الإحتيال بواسطة الوسائل التقنية، أو تجاوز الصلاحية أو إتلاف سرية المعلومات أثناء الإرسال غير العام للبيانات وأثناء إنتقال البيانات من وإلى أو داخل منظومة الكمبيوتر؛

ب) التعمد في إدخال، أو تغيير، أو حذف بيانات الكمبيوتر، مما يؤدى إلى بيانات زائفة بقصد أن يتم النظر فيها أو إتخاذ إجراءات بشأنها لأغراض قانونية كما لو كانت أصلية، بغض النظر عما إذا كانت البيانات واضحة ومقروءة ام لم تكن. يجوز لأي طرف أن يطالب بوجود نية للإحتيال، أو نوايا غير شريفة مماثلة، قبل تولي المسؤولية الجنائية؛

ج) إستخدام البيانات التي تم الحصول عليها من نظام الكمبيوتر عن طريق الإحتيال مع الدراية التامة بذلك؛

د) شراء عن طريق الإحتيال لمصلحة شخص أو أي شخص آخر، أي فائدة من خلال إدخال، أو تعديل أو حذف أو إخفاء بيانات محوسبة أو أي شكل آخر من أشكال التدخل على أداء نظام الكمبيوتر؛

هـ) أية معالجة أو السماح لمعالجة بيانات ذات طابع شخصي، حتى لو كان ذلك بسبب الإهمال، دون الإمتثال للإجراءات الأولية للمعالجة؛

و) المشاركة في تشكيل جمعية أو في إتفاقية مبرمة بهدف إعداد أو إرتكاب جريمة أو أكثر من الجرائم المنصوص عليها بموجب هذه الإتفاقية.

3. الجرائم ذات الصلة بالمحتوى

1. تلتزم الدول الأطراف بإتخاذ التدابير التشريعية و/أو التنظيمية اللازمة لجعل الأفعال التالية جرائم جنائية:

أ) إنتاج وتسجيل أو عرض أو تصنيع أو توفير أو نشر ونقل صورة أو تمثيل المواد الإباحية الخاصة بالأطفال أو أي إنتاج من المواد الإباحية الخاصة بالأطفال عن طريق منظومة الكمبيوتر؛

ب) الشراء للحيازة أو لصالح شخص آخر، أو الشروع في الإستيراد أو الإستيراد، أو الشروع في التصدير أو التصدير لصورة أو تمثيل المواد الإباحية الخاصة بالأطفال عن طريق منظومة الكمبيوتر؛

ج) إمتلاك صورة أو تمثيل المواد الإباحية الخاصة بالأطفال في منظومة الكمبيوتر أو علي وسائل تخزين بيانات الكمبيوتر؛

د) تسهيل أو منح حق الوصول إلى الصور والوثائق والأصوات أو أي تمثيل مواد إباحية لقاصر؛

هـ) إنتاج، وتحميل، ونشر أو إتاحة، بأي شكل من الأشكال، الكتابات، والرسائل، والصور، والرسومات أو أي تمثيل آخر للأفكار أو النظريات العنصرية أو المتعلقة بكراهية الأجانب بواسطة منظومة الكمبيوتر؛

و) التهديد، من خلال نظام الكمبيوتر، بقصد إرتكاب جريمة جنائية ضد أي شخص لأسباب تتعلق بإنتماءه إلي مجموعة تتميز بالعرق أو اللون أو النسب أو الأصل القومي أو الديني حيث تستخدم هذه العضوية كذريعة لأي من هذه العوامل، أو ضد مجموعة من الأشخاص الذين يتميزون بمثل هذه الخصائص.

ز) إهانة، بواسطة نظام كمبيوتر، أي أشخاص لأسباب تتعلق بإنتماءهم إلي مجموعة متميزة بالعرق أو اللون أو النسب أو الأصل القومي أو الإثني أو الدين أو الرأي السياسي، إذا ما أستخدم كذريعة لأي من هذه العوامل، أو ضد مجموعة من الأشخاص الذين يتميزون بمثل هذه الخصائص؛

ح) الإنكار المتعمد، أو الموافقة أو تبرير الأفعال التي تعتبر إبادة جماعية أو جرائم ضد الإنسانية من خلال نظام الكمبيوتر.

2. تتخذ الدول الأطراف التدابير التشريعية و/ أو التنظيمية اللازمة لجعل الجرائم المنصوص عليها بموجب هذه الإتفاقية جرائم جنائية. عندما ترتكب هذه الجرائم تحت رعاية منظمة إجرامية، سوف تخضع هذه الجماعة للعقوبة القصوى المقررة للجريمة.

3. تلتزم الدول الأطراف بإتخاذ ما يجب من تدابير تشريعية و/أو تنظيمية لضمان، أنه في حالة الإدانة، تصدر المحاكم الوطنية أمرا بمصادرة المواد والمعدات والأدوات وبرامج الحاسوب وكافة الأجهزة الأخرى أو البيانات المتعلقة بالشخص المدان، والتي إستخدمت الإرتكاب أي من الجرائم المذكورة في هذه الإتفاقية.

4. الجرائم المتعلقة بإجراءات تأمين الرسائل الإلكترونية

تلتزم الدول الأطراف بإتخاذ ما يجب من تدابير تشريعية و/أو تنظيمية لضمان أن الأدلة الرقمية في القضايا الجنائية مقبولة لإقامة الإدعاء بإرتكاب الجريمة بموجب القوانين الجنائية الوطنية، شريطة أن يكون قد تم عرض هذه الأدلة أثناء الإجراءت ومناقشتها أمام القاضي، وأن الشخص المصدر يمكن تحديده على النحو المطلوب وإن الدليل المذكور قد تم إعداده وحفظه تحت ظروف تضمن سلامته.

المادة 30

مواءمة جرائم معينة إلي تكنولوجيا المعلومات والإتصالات

1. جرائم الممتلكات

أ) تلتزم الدول الأطراف بإتخاذ التدابير التشريعية و/أو التنظيمية لتجريم إنتهاك الممتلكات مثل السرقة والإحتيال وحيازة بضائع مسروقة، وإساءة إستخدام الثقة وإبتزاز الأموال والإبتزاز المتعلق ببيانات الكمبيوتر؛

ب) تلتزم الدول الأطراف باتخاذ ما يلزم من تدابير تشريعية و/ أو تنظيمية لإعتبارها ظروفا مشددة للعوقبة، عندما يتم إستخدام تكنولوجيا المعلومات والإتصالات من أجل إرتكاب جرائم مثل السرقة والإحتيال وحيازة بضائع مسروقة، وإساءة إستخدام الثقة وإبتزاز الأموال والإرهاب، وغسل الأموال؛

ج) تلتزم الدول الأطراف بوضع ما يلزم من تدابير تشريعية و/ أو تنظيمية تشمل علي وجه التحديد "**بواسطة وسائل الإتصال الإلكترونية الرقمية**" مثل الإنترنت في سرد وسائل النشر العام المنصوص عليها في القانون الجنائي للدول الأطراف؛

د) تلتزم الدول الأطراف باتخاذ ما يجب من التدابير التشريعية الجنائية اللازمة لتقييد الوصول إلى الأنظمة المحمية التي تم تصنيفها علي أنها تمثل البنية التحتية للدفاع الوطني حيث أنها تحتوي على البيانات الحساسة المتعلقة بالأمن القومي.

2. المسؤولية الجنائية للأشخاص الإعتباريين

تلتزم الدول الأطراف بإتخاذ مايجب من التدابير التشريعية اللازمة لضمان أن تتحمل الشخصيات الإعتبارية غير الدولة، المجتمعات المحلية والمؤسسات العامة المسؤولية عن الجرائم المنصوص عليها في هذه الإتفاقية، التي ترتكب نيابة عنها من قبل أعضائها أو ممثليها. إن مسؤولية الأشخاص الإعتباريين لا تستبعد مسئولية الأشخاص الطبيعيين الذين هم مرتكبي أو شركاء في نفس الجرائم.

المادة 31

مواءمة بعض العقوبات لتكنولوجيا المعلومات والإتصالات

1. العقوبات الجنائية

أ) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أن الجرائم المنصوص عليها في هذه الإتفاقية يعاقب عليها بعقوبات جنائية فعالة ومناسبة ورادعة؛

ب) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أن الجرائم المنصوص عليها في هذه الإتفاقية يعاقب عليها بالعقوبات المناسبة بموجب تشريعاتها الوطنية؛

ج) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أن الشخص الإعتباري الذي تم تحميله المسؤولية، بموجب بنود هذه الإتفاقية، يعاقب عليها عقوبات ناجعة ومناسبة ورادعة بما في ذلك الغرامات الجنائية.

2. العقوبات الجنائية الأخرى

أ) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أنه في حالة الإدانة بجريمة إرتكبت عن طريق وسيلة إتصال رقمية، يجوز للمحكمة المختصة إنزال عقوبات إضافية؛

ب) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أنه في حالة الإدانة بجريمة إرتكبت عن طريق وسيلة إتصال رقمية، فانه يجوز للقاضي أن يأمر بالإضافة، علي حساب

الشخص المدان، بنشر إلزامي لمقتطف من الحكم، عبر نفس الوسائل، وفقاً للطرق المنصوص عليها في قوانين الدول الأعضاء؛

ج) تلتزم الدول الأطراف باتخاذ التدابير التشريعية اللازمة لضمان عدم الإخلال بسرية البيانات المخزنة في نظام الكمبيوتر ويستوجب ذلك نفس العقوبات المطبقة على خروقات السرية المهنية.

3. القانون الإجرائي

أ) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أنه إذا كانت البيانات المخزنة في نظام الكمبيوتر أو في أي وسيلة تسمح لتخزين البيانات المحوسبة في أراضي الدولة الطرف، قد تفيد في إجلاء الحقيقة، فإنه يمكن للمحكمة المعنية القيام بالبحث، بغرض الوصول إلى نظام الكمبيوتر أو جزء منه بواسطة نظام كمبيوتر آخر حيث أن البيانات المذكورة يمكن الوصول إليها عن طريق، أو متاحة في، النظام الأولي؛

ب) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أنه في حالة إكتشاف السلطة القانونية المسؤولة عن التحقيق أن البيانات المخزنة في نظام الكمبيوتر هي مفيدة لإقامة الحقيقة، ولكن يبدو أن الإستيلاء عليها لم يكن مناسبا، فإن البيانات المذكورة وكذلك جميع البيانات المطلوبة لفهمها، يجب نسخها إلى وسيلة تخزين بيانات الكمبيوتر حيث يتم ضبطها وإحكام إغلاقها، وفقا للطرق المنصوص عليها في تشريعات الدول الأطراف؛

ج) تتخذ الدول الأطراف التدابير التشريعية اللازمة لضمان أن السلطات القضائية، لأغراض التحقيق أو تنفيذ الإنابة القضائية، سوف تقوم بتنفيذ العمليات المنصوص عليها في هذه الإتفاقية؛

د) تلتزم الدول الأطراف بوضع التدابير التشريعية اللازمة لضمان أنه، وإذا كانت ضرورة المعلومات تملي ذلك، وعلي وجه الخصوص إذا كانت هناك أسباب تدعو للإعتقاد بأن المعلومات المخزنة في نظام كمبيوتر هي عرضة بشكل خاص للفقدان أو التعديل، فان لقاضي التحقيق أن يصدر أمرا قضائيا لأي شخص لصون وحماية سلامة البيانات التي في حوزته أو تحت سيطرته، لمدة لاتزيد عن عامين، وذلك لضمان حسن سير التحقيق. وأي شخص يؤتمن على هذه البيانات أو أي شخص آخر مسؤول عن الحفاظ على هذه المعلومات، عليه ضمان الحفاظ على سرية البيانات؛

ه) تتخذ الدول الأطراف التدابير التشريعية اللازمة لضمان، أن قاضي التحقيق يمكنه، عند الاقتضاء، إستخدام الوسائل التقنية المناسبة للقيام في حينها، بجمع أو تسجيل البيانات المتعلقة بمحتويات إتصالات خاصة في أراضيه، ونقلها عن طريق نظام الكمبيوتر أو إجبار مزود الخدمة،

في إطار قدراته التقنية، على جمع وتسجيل البيانات، وذلك بإستخدام التسهيلات التقنية الموجودة في أراضيه أو الدول الأطراف، أو تقديم الدعم والمساعدة إلي السلطات المختصة من أجل جمع و تسجيل تلك البيانات المحوسبة.

الفصل 4

الأحكام الختامية

المادة 32

التدابير الواجب إتخاذها على مستوى الإتحاد الأفريقي

علي رئيس مفوضية الإتحاد الأفريقي أن يقدم تقريرا لرؤساء الدول والحكومات الأفريقية بشأن إنشاء ورصد الآلية التنفذية لهذه الإتفاقية .

وستسعى آلية الرصد المقرر إنشاؤها إلى تحقيق ما يلي:

أ) تعزيز وتشجيع القارة الأفريقية علي إعتماد وتنفيذ تدابير لتعزيز أمن الفضاء الإلكتروني في الخدمات الإلكترونية وفي مكافحة الجريمة الإلكترونية وإنتهاكات حقوق الإنسان في الفضاء الإلكتروني؛

ب) جمع الوثائق والمعلومات بشأن إحتياجات أمن الفضاء الإلكتروني وكذلك حول طبيعة وحجم الجريمة الإلكترونية وإنتهاكات حقوق الإنسان في الفضاء الإلكتروني؛

ج) العمل علي وضع الطرق لتحليل إحتياجات أمن الفضاء الإلكتروني وحول طبيعة وحجم الجريمة الإلكترونية وإنتهاكات حقوق الإنسان في الفضاء الإلكتروني، ونشر المعلومات وتوعية الجمهور بشأن الآثار السلبية لهذه الظواهر؛

د) تقديم المشورة للحكومات الأفريقية بشأن أفضل السبل لتعزيز أمن الفضاء الإلكتروني ومكافحة آفة الجريمة الإلكترونية وإنتهاكات حقوق الإنسان في الفضاء الإلكتروني على المستوى الوطني؛

هـ) جمع المعلومات وإجراء التحاليل حول السلوك الإجرامي لمستخدمي شبكات المعلومات وأنظمة الكمبيوتر العاملة في أفريقيا، ونقل هذه المعلومات إلى السلطات الوطنية المختصة؛

و) صياغة وتشجيع إعتماد مدونات قواعد السلوك لتكون مواءمة، للإستخدام من قبل الموظفين العموميين في مجال أمن الفضاء الإلكتروني؛

ز) إقامة شراكات مع المفوضية والمحكمة الأفريقية لحقوق الإنسان والشعوب، والمجتمع المدني الأفريقي، والمنظمات الحكومية، والمنظمات الحكومية الدولية والمنظمات غير الحكومية بغية

تسهيل الحوار بشأن مكافحة الجريمة الإلكترونية وإنتهاكات حقوق الإنسان في الفضاء الإلكتروني؛

ح) تقديم تقارير منتظمة إلى المجلس التنفيذي للإتحاد الأفريقي حول التقدم الذي أحرزته كل دولة طرف في تنفيذ أحكام هذه الإتفاقية؛

ط) القيام بأي مهام أخرى تتعلق بالجريمة الإلكترونية وإنتهاكات حقوق الأفراد في الفضاء الإلكتروني والتي قد تسند إليها من قبل أجهزة صنع السياسات في الإتحاد الأفريقي.

المادة 33
أحكام الحماية

لايجوز تفسير أحكام هذه الاتفاقية على نحو يتعارض مع مبادئ القانون الدولي ذات الصلة، بما في ذلك القانون الدولي العرفي.

المادة 34
تسوية المنازعات

1- يتم تسوية أي نزاع ينشأ عن هذه الإتفاقية وديا عن طريق المفاوضات المباشرة بين الدول الأطراف المعنية.

2- حيث لا يمكن حل النزاع عن طريق المفاوضات المباشرة، يتعين على الدول الأطراف أن تسعى الى تسوية النزاع بالوسائل السلمية الأخرى، بما في ذلك المساعي الحميدة والوساطة والتراضي، أو بأي وسيلة سلمية أخرى تتفق عليها الدول الأطراف. وفي هذا الصدد، ينبغي تشجيع الدول الأطراف على الاستفادة من إجراءات وآليات تسوية المنازعات التي أنشأت في إطار الإتحاد.

المادة 35
التوقيع أو التصديق أو الإنضمام

تكون هذه الإتفاقية مفتوحة لجميع الدول الأعضاء في الإتحاد، للتوقيع أو التصديق أو الإنضمام، وفقا للإجراءات الدستورية لكل منها.

المادة 36

الدخول حيز النفاذ

تدخل هذه الإتفاقية حيز التنفيذ بعد ثلاثين (30) يوما من تاريخ إستلام رئيس مفوضية الإتحاد الأفريقي صك التصديق الخامس عشر (15) .

المادة 37

التعديل

1- يجوز لأي دولة طرف تقديم مقترحات لتعديل هذه الإتفاقية أو إعادة النظر فيها.

2. يجب تقديم مقترحات التعديل أو المراجعة إلى رئيس مفوضية الإتحاد الأفريقي، الذي يقوم بدوره بإحالتها إلى الدول الأطراف في غضون ثلاثين (30) يوما من إستلامها.

3. يبحث مؤتمر الإتحاد، بناء على توصية من المجلس التنفيذي للإتحاد، هذه المقترحات في دورته المقبلة، بشرط أن يتم إخطار جميع الدول الأطراف قبل ثلاثة (3) أشهر على الأقل من بداية الدورة.

4. يقوم مؤتمر الإتحاد بإعتماد التعديلات وفقا لقواعد اجراءاته .

5. تدخل التعديلات أو التنقيحات حيز النفاذ وفقا لأحكام المادة 36 أعلاه.

المادة 38

الإيداع

1- تودع صكوك التصديق أو الإنضمام لدى رئيس مفوضية الإتحاد الأفريقي؛

2 - يجوز لأي دولة طرف أن تنسحب من هذه الإتفاقية بايداع إشعار خطي مقدما قبل ذلك بعام واحد (1) إلى رئيس مفوضية الإتحاد الأفريقي.

3 - يقوم رئيس مفوضية الإتحاد الأفريقي بإخطار الدول الأعضاء بأي توقيع، أو إيداع أي صك للتصديق أو الإنضمام الى هذه الإتفاقية، وكذلك دخولها حيز النفاذ.

4 - يقوم رئيس المفوضية أيضا بإخطار الدول الأطراف بأي طلبات للتعديل أو الإنسحاب من الإتفاقية، فضلا عن التحفظات بهذا الشأن.

5 - عند بدء نفاذ هذه الإتفاقية، يقوم رئيس المفوضية بتسجيلها لدى الأمين العام للأمم المتحدة، وفقا للمادة 102 من ميثاق الأمم المتحدة.

6 - حررت هذه الإتفاقية، في أربعة (4) نصوص أصلية باللغات العربية والإنجليزية والفرنسية والبرتغالية، وجميع النصوص الأربعة (4) متساوية الحجية،ويجب ان تودع لدى رئيس المفوضية الذي يقوم بدوره بإرسال نسخة أصلية معتمدة من الإتفاقية إلى كل دولة عضو في الإتحاد الأفريقي بلغتها الرسمية .

تم إعتمادها في الدورة العادية الثالثة والعشرون
لقمة رؤساء دول وحكومات الإتحاد الأفريقي المنعقدة في ملابو، غينيا الإستوائية،
27 يونيو 2014.

نسخة مطابقة لأصل النص
كما وافق عليه مجلس المستشارين