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

الأمانة العامة للحكومة (المطبعة الرسمية) - الرباط 2021 - 1442

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 والتوجهات 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 بب 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 سواء 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 اي 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 الإشـارات 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؛

الجهـاز الإلكترونـي للتحقـق مـن التوقيـع: يعني مجموعة من البرمجيات أو الأجهزة التي تسمح بالتحقق من التوقيع الإ لكتروني؛

الجهـاز الإلكترونـي لإنشـاء التوقيـع: يعني مجموعة من البرمجيات أو الأجهزة التي تسمح بإنشاء التوقيع الإلكتروني؛

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

تجـاوز النفـاذ المسموح بـه: 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 السيكولوجية 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 على 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 التي يوجد في 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 المعنوي الذي 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 الذي 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 في 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 الطبيعي 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 التي 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 خاضعةً 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 السكاني؛

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 علي 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؛

ه) 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؛