



# استخدام الإنترنت في كامل الأمان

حسن استعمال الشباب والأطفال للفضاء الرقمي

وثيقة من إعداد مجموعة العمل الخاصة بموضوع  
التقنين ووسائل الإعلام الرقمية



الهيئة العليا للاتصال السمعي البصري  
Haut Autorité de la Communication Audiovisuelle





”من الملح وضع جهاز للبيقطة الرقمية ومد الأطفال والشباب  
وأولياء أمرهم بالأدوات اللازمة للإبحار في الفضاء الرقمي،  
ذلك المحيط اللامتناهي والذي لا يخلو من مخاطر”  
مجموعة العمل الخاصة بموضوع «التقنين ووسائل الإعلام الرقمية»







## قائمة المحتويات



- معجم
- مقدمة
- الاتصال المفرط بالإنترنت والإدمان على الشبكة الرقمية
- كيف نتعرف على الإدمان الرقمي عند الأطفال؟
- تأثير التأقلم مع نظام التمدرس عن بعد
- التحديات الرقمية التي تستهدف الشباب
- التحديات في مواقع التواصل الاجتماعي: المخاطر المحدقة بالصحة
- الاعتداء الجنسي على الأطفال واستغلالهم في إنتاج المواد الإباحية والتحرش الرقمي
- كيف نحمي الأطفال من المتحرشين على شبكة الإنترنت؟
- المعطيات الشخصية: ما السبيل لحمايتها؟
- الممارسات الفضلى من أجل تدبير فعال لمعطياتكم الشخصية
- كيف تقوم بتدقيق المعلومات بمفردك؟
- توصيات



## معجم

**التزييف العميق:** تقنية صنع فيديوهات مزيفة من خلال تعديل محتوى الفيديو أو التلاعب فيه ليظهر لأول وهلة كأنه حقيقي بشكلٍ كبير جداً. وتعتمد هذه التقنية أساساً على تكنولوجيا الذكاء الاصطناعي، حيث تقوم بدمج مجموعة صور ومقاطع فيديو وتسجيلات صوتية لشخص معين لإنتاج مقطع فيديو جديد يقول فيه الشخص كلاماً غير حقيقي أو يقوم بتصرفات لم يقر بها في الواقع.

**تدقيق الحقائق:** عملية تتمثل في التأكد من مدى صحة ودقة الأخبار والمعلومات المروج لها في الفضاء الرقمي، حيث توجد العديد من البرامج والمنصات التي تسهر على هذه العملية.

**لعبة «بيجي» PUBG:** صدرت هذه اللعبة في 23 مارس 2017 على أجهزة الكمبيوتر، ثم لقيت نجاحاً كبيراً بعد انتشارها عام 2018 عبر الهواتف الذكية. وتعتبر PUBG لعبة قتالية تقوم على قاعدة «البقاء للأقوى»، حيث تبدأ بمائة لاعب لتنتهي بفوز لاعب أو فريق واحد. كما أنها لعبة مجانية تجمع لاعبين من مختلف دول العالم بساحة للقتال، وتتيح لهم مجانية التحدث لوقت غير محدد، إلا أنها تحولت خلال الفترة الأخيرة من وسيلة للمتعة إلى منصة للقتل وسببت العديد من الانتحارات عبر العالم.

**الاستغلال الإباحي للأطفال:** استغلال الأطفال والقاصرين في إنتاج المواد الإباحية.

**التحرش عبر الإنترنت:** استخدام شبكة الإنترنت بغرض التنمر أو إيذاء الأشخاص بشكل متعمد ومتكرر وعدائي.

**الاعتداء الجنسي على الأطفال:** هو جريمة ذات طبيعة جنسية يقترفها شخص بالغ إزاء الأطفال. ويشمل هذا الفعل التحرش الجنسي بالأطفال واستغلال القاصرين في إنتاج المواد الإباحية وغيرها من الممارسات المسيئة لكرامة الطفل واتزانه الصحي.

**الرقابة الأبوية:** تتمثل في وضع الوالدين أو أولياء الأمر لبرنامج معلوماتي داخل أجهزة أطفالهم الموصولة بالإنترنت لمراقبة نشاطهم الرقمي أو منعهم من الولوج إلى المواقع غير اللائقة.

**ملفات تعريف الارتباط:** هي ملفات يمكن تخزينها على جهاز الحاسوب الخاص بك أو غيره من الأجهزة الموصولة بالإنترنت عند زيارة موقع إلكتروني ما. وتستخدم هذه الملفات لتتبع نشاطك داخل المواقع الإلكترونية وتحسين تجربة التصفح الخاصة بك وتقديم إعلانات موجهة.

**الإعلانات الموجهة:** تعمل تقنية الإعلانات الموجهة على رصد وتتبع أثر مستخدمي الإنترنت وتحليل نشاطهم الرقمي للتعرف على اهتماماتهم ورغباتهم وعرض إعلانات تناسبهم.



**إعادة الاستهداف:** هي عملية تدرج ضمن استراتيجيات التسويق الإلكتروني، حيث تتمثل في إعادة استهداف الأشخاص الذين سبق لهم وأن أبدوا اهتمامهم بمنتج أو خدمة ما، وذلك عن طريق إعلانات موجهة تظهر لهم أثناء تصفحهم للإنترنت. ويتم استهداف تلك الفئة من الأشخاص والتعرف عليهم بالاعتماد على ملفات تعريف الارتباط.

**البيانات الوصفية:** هي معلومات تستخدم لوصف البيانات الموجودة في صفحة ويب أو مستند أو ملف.

**الشبكة الافتراضية الخاصة:** هي إحدى التقنيات التي تسمح للمستخدمين عن بعد بإنشاء اتصال آمن بشبكة خاصة.

**النظام العام لحماية البيانات:** مجموعة من القواعد والقوانين تم وضعها من قبل الإتحاد الأوروبي لحماية حقوق وخصوصية الأفراد داخل الإتحاد الأوروبي.





## مقدمة

بات الفضاء الرقمي اليوم الزاوية الرئيسية والمعلم الأساس لفهم الثقافة وتطويرها. فلا جدال في أن ثقافة الإعلام، أو ثقافة السمعى البصرى بمنظور أوسع، تعتبر في وقتنا الراهن رقمية بامتياز. وينبغى علينا اليوم تسليط الضوء على مفهوم الثقافات الرقمية، الذي يكشف عن تنوع الثقافات داخل الفضاء الرقمية. كما يجب الإقرار بأن شبكة الإنترنت قد أصبحت حقيقة اجتماعية تؤثر بشكل واضح على أنماط استهلاكنا للمعلومة والصورة والصوت.

وتعتبر الإنترنت من الدعائم الكبرى للتحوّل الثقافى الذى نشهده اليوم، خاصة وأن التقنيات التى يزخر بها هذا الفضاء الرقمية غير المحدود ( والذى ظل طويلا دون حواجز) غيرت كليا علاقتنا مع العالم من حولنا ومع الآخر وكل ما هو «مقروء ومرئى ومسموع».

تقع مسؤولية حماية الشباب والأطفال في صلب اهتمامات هيئة التقنين، لا سيما وأنهم معرضون بشكل كبير لهذه الثقافات الرقمية التى تتجدد قواعدها ومعاييرها باستمرار، والتي تنتقل عبر المنصات الرقمية والمواقع الاجتماعية. لا يكون الآباء والأمهات بالضرورة على علم بكل ما يجرى لأبنائهم حين يظنون بمفردهم أمام الشاشات. وحتى عندما يكونون على معرفة بذلك، فهم لا يدركون حقا جدية الأمر.

يقوم شباب (صغار سنا في غالب الأحيان) بفتح قنوات باسمهم والاشتراك في قنواتهم المفضلة ونشر محتويات يتصورون فيها والتعبير عن الشكر لمشركيهم وتشجيعهم على ترك تعليقاتهم، كما يتواصلون مع أشخاص مجهولى الهوية من شتى بقاع العالم. ويتيح الفضاء الرقمية للأطفال فرصة التعبير بحرية تامة وبمعزل عن وصاية الكبار.

وفي هذا الصدد، من الملح وضع جهاز لليقظة الرقمية ومد الأطفال والشباب وأولياء أمرهم بالأدوات اللازمة للإبحار في الفضاء الرقمية، ذلك المحيط اللامتناهى والذي لا يخلو من مخاطر.

«استخدام الإنترنت في كامل الأمان»، هو الهدف الرئيسى لهذا الدليل الذى تم إعداده في إطار مجموعة العمل الخاصة بموضوع التقنين ووسائل الإعلام الرقمية. فهو يقدم أدوات لتطوير مهارة التحقق من الخبر والكشف عن المحتويات غير اللاتقة وحماية المعطيات الشخصية وكذا بعض الآليات لتجنب التعرض للإدمان الرقمية. كيف ينتقل المحتوى الذى تتم مشاركته في موقع اجتماعى ما؟ وماذا نقصد بالأخبار الزائفة؟ هل تعتبر تقنية التزييف العميق تلاعبا في الصورة؟ وهل يمكن للتحديات التى تنتشر في الفضاء الرقمية أن تشكل خطرا على الأطفال والشباب؟

يقدم هذا الدليل أجوبة ويقترح آليات لليقظة الرقمية ويعرض حلولاً لضمان تصفح (تقريباً) دون مخاطر بالنسبة للأطفال وأولياء أمرهم. كما يعتمد على رسومات لتوضيح ضرورة الحوار المبني على الثقة التامة بين الأطفال وآبائهم، وقدوة الكبار، وخلق فضاءات خالية من الشاشات في المنزل. تتمى لكم قراءة ممتعة ومفيدة من أجل استخدام الإنترنت في كامل الأمان .

نرجس الرغاي

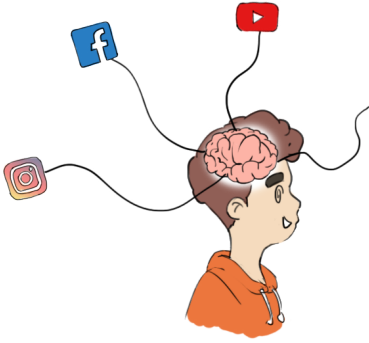
عضوة بالمجلس الأعلى للاتصال السمعى البصرى

رئيسة مجموعة العمل الخاصة بموضوع « التقنين ووسائل الإعلام الرقمية »



## الفصل 1

# الاتصال المفرط بالإنترنت والإدمان على الشبكة الرقمية



- الاتصال بالإنترنت هو أن يكون لديك رابط مع العالم. كما أن الولوج إلى التكنولوجيا عامل للتنمية على عدة مستويات؛
- يساهم الاتصال بالإنترنت في الحد من التفاوتات في الوصول إلى المعلومة والاستفادة من المعرفة؛
- لا يهدف هذا الدليل إلى تشويه أنماط الاتصال الرقمي عند الشباب والأطفال، بل إلى التحسيس بالآثار التي قد يخلفها استخدامهم المفرط للإنترنت؛
- الاتصال بالإنترنت له معنى إيجابي!

## التعرض للشاشات لفترات طويلة

تفيد الدراسة التي أصدرتها الوكالة الوطنية لتقنين المواصلات سنة 2020 حول تكنولوجيا المعلومات والاتصال بالمغرب ما يلي:



يتوفر 89.7% من الأطفال المتراوح أعمارهم ما بين 5 سنوات و14 سنة على هاتف نقال، ولدى 85.5% منهم هاتف ذكي. يستعمل 80.5% من هذه الفئة العمرية شبكة الإنترنت، حيث يتصل 75.6% منهم بالإنترنت على الأقل مرة واحدة في اليوم. 97.9% منهم يستخدمون مواقع التواصل الاجتماعي.

\* للاطلاع على الدراسة التي أصدرتها الوكالة الوطنية لتقنين المواصلات سنة 2019 حول تكنولوجيا المعلومات والاتصال بالمغرب، يمكن زيارة الموقع: [https://www.anrt.ma/sites/default/files/publications/enquete-tic-\\_2019-fr.pdf](https://www.anrt.ma/sites/default/files/publications/enquete-tic-_2019-fr.pdf)



## أوضحت دراسة المندوبية السامية للتخطيط (الصادرة سنة 2018) حول المؤشرات الاجتماعية ما يلي:



تحظى التلفزة بنسبة 43.6% من وقت فراغ الأطفال البالغين من العمر أقل من 15 سنة، أي ما يعادل 3 ساعات في اليوم.

يخصص الأطفال المغاربة دقيقتين فقط لممارسة الرياضة ودقيقة واحدة للقراءة في اليوم.



تجدر الإشارة كذلك إلى أن الأطفال يقضون 12 دقيقة على شبكة الإنترنت، أي 4 دقائق أزيد من المعدل المسجل لدى الكبار (8 دقائق). وتتغير هذه المدة الزمنية من 21 دقيقة في الوسط الحضري إلى دقيقتين في الوسط القروي. يستخدم الأطفال الإنترنت في أغلب الأحيان للاتصال بمواقع التواصل الاجتماعي، فيما تمثل الحصة المخصصة للأبحاث المدرسية 5% فقط.





## انجذاب الأطفال الصغار إلى الشاشات منذ سن مبكرة



ينجذب الأطفال بشكل تلقائي إلى الشاشات إلى أن يصبحوا مخدرين تقريبا عندما توضع أمام أيديهم. صارت الشاشة حلا لكل شيء، فهي أداة لتلهية الطفل أو تهدئته أو مراقبته. وتكون النتيجة أن ينمو الأطفال بين زجاجة الرضاعة والشاشات. اهتمت دراسات أولية بالتأثير العصبي والنفسي لاستعمال الأطفال الصغار للشاشات.

وأوضحت أن تعرضهم للشاشات له انعكاسات سلبية على نمو الدماغ وتعلم المهارات الأساسية. كما أنهم الأكثر تعرضا لمخاطر التأخر اللغوي بسبب النظر المطول إلى الشاشات.





## كيف نتعرف على الإدمان الرقمي عند الأطفال؟

بعض الإشارات كتبين احتمال وجود إدمان عند الطفل



**1** لا يتحكم الطفل في الوقت المستغرق أمام الشاشة ويطلب بالمزيد؛



**2** عند توجيه ملاحظة إليه، يبقى في وضعية إنكار أو يقلل من جدية الأمر؛



**3** يتصرف بعنف عندما لا يكون متصلا بالإنترنت؛



**4** يحس الطفل بالفراغ والإحباط عندما يفارق الشاشات ولا يعبر عن أدنى اهتمام بالأنشطة الأخرى، حتى تلك التي كان يستمتع بها من قبل؛

**6** ينطوي على نفسه ويفضل المحادثات الافتراضية على الواقعية...

**5** يصبح قلقا وتعبا باستمرار ويقل حبه للاستطلاع وتركيزه وتراجع نتائجه في المدرسة...



## الأطفال والشاشات: مسؤوليتنا جميعا



عندما يكون الطفل في مرحلة صقل مهاراته وتطوير حواسه الخمس، يجعله التعرض السلبي للصور المبتوثة على الشاشات مجرد مشاهد يطاوع كل ما يتلقاه، مما «قد» يؤثر «في بعض الحالات» على نموه، بل أخطر من ذلك على وظائفه الإدراكية من الحفظ والانتباه والحركة.

قد يترك استعمال الأطفال للشاشات في سن مبكرة آثارا وخيمة على صحتهم، إذ يصبح نومهم مضطربا ويزيد وزنهم بسبب انعدام الحركة ويعانون من مشاكل حادة على مستوى البصر.



## توصيات منظمة الصحة العالمية بشأن استعمال الأطفال للشاشات: اعتماد هذه الإرشادات بدون قيود



عدم الجلوس أمام الشاشات إطلاقاً بالنسبة للأطفال دون العامين.  
ينصح بشدة تعودهم على قراءة القصص وممارسة الأنشطة البدنية؛

عدم قضاء الأطفال الذين يتجاوز عمرهم العامين أكثر من ساعة واحدة يومياً في مشاهدة التلفزيون أو الفيديوهات أو ممارسة ألعاب الحاسوب. ينصح تعودهم على قراءة القصص وممارسة الأنشطة البدنية؛



رغم توفر السوق على العديد من الأسطوانات التعليمية والألعاب التربوية على الشاشة، إلا أنه يجب استعمالها فقط في بعض الأوقات، تكميلاً للألعاب الكلاسيكية المعروفة (تركيب الصور المقطوعة وألعاب المكعبات وقطع البناء)؛

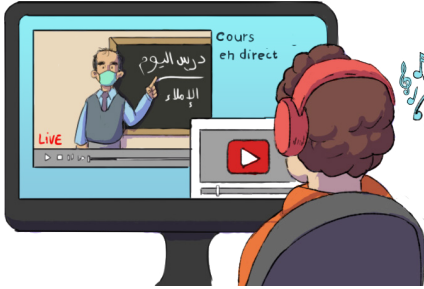
المراقبة الأبوية لمدة استعمال الأطفال للإنترنت وطبيعة اتصالهم الرقمي ضرورة ملحة لضمان استخدام صحي وآمن للشاشات.



## تأثير التأقلم مع نظام التمدرس عن بعد

### مع نظام التعلم عن بعد، ظهر نمط جديد للاتصال بالإنترنت

صدرت قواعد جديدة عن الحجر الصحي الذي فرضته تدابير محاربة فيروس كورونا المستجد: لتعلم وإيصال المعرفة، من الضروري أن نبقى متصلين بالإنترنت. وقد حلت الحواسيب والهواتف والألواح محل السبورة.



يبقى الأطفال وصغار الشباب متصلين بالإنترنت في منازلهم على مدار الساعة بحجة أنهم يدرسون عن بعد. فهل يخلو الانعزال للاتصال بالإنترنت من المخاطر في زمن كورونا ؟

## ما هي الحلول التي ينبغي اعتمادها لتحقيق اتصال رقمي ملائم لا يتحول إلى إدمان؟



### صندوق الأدوات

توجد العديد من التقنيات البسيطة جدا للحد من هذا الإدمان:

#### 1 قدرة الوالدين

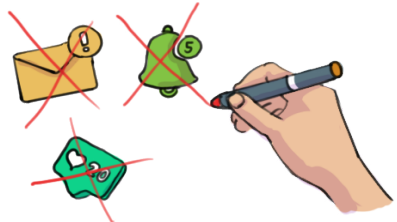
يشكو الوالدين من إدمان أطفالهم على الشاشات، فيما يقضون هم أنفسهم معظم الوقت أمامها. النصيحة الأولى لمرافقة الشباب والأطفال في استخدامهم للإنترنت هي أن تتحكم نحن أولا في الزمن المستغرق أمام الشاشة.



#### 2 تعطيل الإخطارات

ينبغي تعطيل إخطارات تطبيقات الهاتف للحد من الضغط غير المستحب.

يمكن كذلك اختيار ما يظهر على الشاشة من إخطارات الواتساب وفيسبوك وتيك توك وأي شبكة اجتماعية أخرى، وذلك للتقليل من الرغبة الملحة في تصفح الهاتف.





### 3 خلق مساحات خالية من الشاشات في المنزل:



يساهم خلق مساحات دون شاشات في تقليل المدة الزمنية المستغرقة أمامها وإرساء عادات جديدة.

امنعوا الأطفال دون العامين كلياً من الجلوس أمام الشاشات، وقللوا قدر الإمكان من استعمالها بالنسبة للأطفال أقل من 5 سنوات، وصاحبوا أطفالكم قبل 10 سنوات في تصفحهم للإنترنت وعلموهم الرقابة الذاتية. وبعد سن العاشرة، انتبهوا لعلامات التعب لديهم وتأثرهم الدراسية.

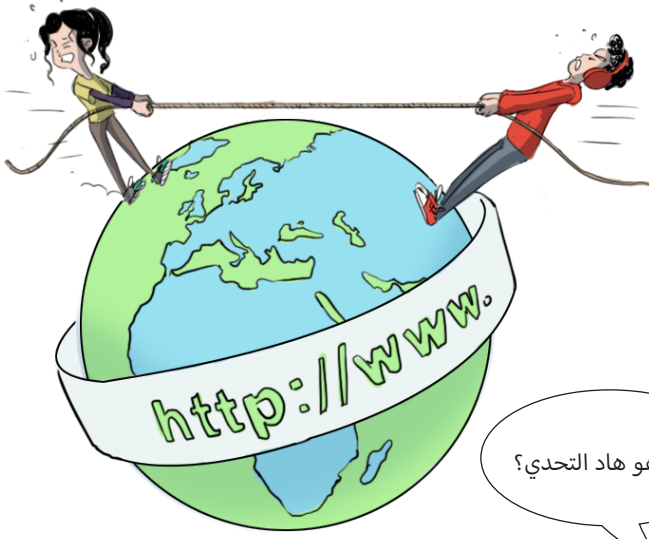
تفيد الإرشادات الجديدة التي أصدرتها منظمة الصحة العالمية سنة 2019 بخصوص صحة الأطفال الصغار أن حظر الشاشات كلياً يكون في سن العامين، حتى أن البعض يفضل منعها بشكل نهائي قبل سن الثالثة.





## التحديات الرقمية التي تستهدف الشباب

الفصل  
2



تنتشر التحديات على شبكة الإنترنت وتسيطر عليها، حيث تمر من مجرد لعبة بين الأصدقاء إلى نهاية مأساوية. تمر التحديات من اللعبة البريئة، التي غالبا ما تكون هزلية، إلى التحدي الخطير الذي يقود إلى كل أنواع الانحرافات، بل حتى إلى الموت. يجري التحدي عموما بين الأصدقاء وتتم مشاركته على شبكات التواصل الاجتماعي، مما يفسر انتشاره الرقمي السريع. وتظهر تحديات جديدة باستمرار على شبكة الإنترنت، حيث تختلف شعبيتها بين الشباب من شخص لآخر. من الضروري توخي الحذر في تلقي هذه المنشورات لأن هؤلاء الشباب والأطفال غالبا ما يشاركون في تلك التحديات بعيدا عن الأنظار وفي سرية تامة داخل غرفهم.



### كيف ظهرت هذه التحديات؟

توجد التحديات والألعاب الخطرة منذ عدة عقود، حيث سُجّلت الممارسات الأولى لهذه الألعاب في خمسينيات القرن الماضي. وقد ساهمت شبكة الإنترنت ومواقع التواصل الاجتماعي بشكل رئيسي في الانتشار السريع لهذه التحديات. فمن خلال التقاط المشاركين للصور وتصويرهم للفيديوهات، يحظون بانتشار كوني وبلا حدود.



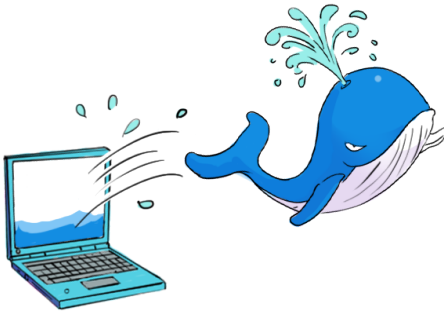
## التحديات في مواقع التواصل الاجتماعي: المخاطر المحدقة بالصحة

ينبغي من باب الاحتياط معرفة أكبر قدر ممكن من المعلومات عن هذه الألعاب الرقمية التي قد تخلّف أضرارا لا يمكن إصلاحها.

ستجدون فيما يلي قائمة سوداء وغير شاملة حول أخطر التحديات الموجودة على الإنترنت. تجدر الإشارة إلى أن الكثير منها لم ينتشر في الفضاء الرقمي المغربي، إلا أن بعضها لقي إقبالا ملحوظا في بلادنا.

### تحدي الحوت الأزرق

ظهر تحدي «الحوت الأزرق» في روسيا سنة 2015، حيث لقي تغطية إعلامية هامة بعد انتحار فتاة شابة بسبب هذه اللعبة. وعُرف هذا التحدي بعد ذلك في معظم بلدان أوروبا ربيع سنة 2017، بعدما نقلت الصحافة العديد من الأخبار المتعلقة بانتحارات راح ضحيتها شباب مراهقون في روسيا جراء هذه التحديات الغامضة التي ظهرت على شبكة الإنترنت. تقوم فكرة «الحوت الأزرق» على اتصال أشخاص غامضين مشرفين على التحديات بالعديد من الأطفال وصغار الشباب عبر مواقع الدردشة السرية، إذ يطلبون منهم القيام بخمسين تحد. وتكون هذه التحديات في البداية بريئة وممتعة، إلى أن تتحول بسرعة فائقة إلى نهاية محتمة تتمثل في الانتحار.



### تحدي النار

يقوم صغار الشباب في «تحدي النار» بصب الكحول أو الوقود أو أي سائل آخر سريع الاشتعال على جزء من جسدھم (الصدر أو الساق أو الذراع...)، ثم يستخدمون الولاعة لإشعال النار... ويقوم الأكثر حذرا منهم بإجراء التحدي في الحمام لكي يطفؤوا النيران بسرعة فور اندلاعها. لكن غالبا ما تقلب الأمور على المشاركين في هذا التحدي، إذ يشتد إحساسهم بالألم ولا يستطيعون فتح صنبور الماء لإخماد النار التي تحرقهم.





## تحدي كسر الجمجمة



تتجلى فكرة هذه اللعبة، التي ظهرت أولاً بفيديو، في أن يقف ثلاثة أطفال في صف واحد، حيث يقفز الطفلان في البداية على يمين ويسار الفتى الأوسط الذي لا يكون على علم بالتحدي. وما إن يأتي دور هذا الأخير ليقفز في الهواء حتى يوجهان له ضربة بالأقدام إلى قصة ساقه فيفقد اتزانَه ويسقط في الأرض بقوه ويقع على ظهره. يتسبب هذا التحدي القاتل، الذي يمارسه الكبار أيضاً، في فقدان الوعي والارتجاج في المخ أو حتى الشلل.

## لعبة الخنق

يعتبر هذا التحدي بمثابة كابوس بالنسبة للآباء والمدرسين، ويقوم به الطفل أو المراهق بمفرده أو يطلب من أحد أصدقائه أن يُلّف حول عنقه ربطة عنق أو وشاح ويشد عليه ليقبس قدرته على التحمل من دون تنفس. وتكون عواقب هذه التجربة المؤلمة أن تخلف عاهات مستديمة أو تقود إلى موت محتم.



مازال ليا  
3 سنتيمتر

رقاقتي بزاف!  
كتباني بحال شي  
هيكل عظمي.

## تحدي ورقة A4

ظهر تحدي ورقة A4 في الصين، حيث تتعاطى له الفتيات بشكل خاص على مواقع التواصل الاجتماعي وله أضرار كبيرة على الصحة. يتمثل هذا التحدي في وضع الفتاة ورقة طباعة A4 أمام خصرها والتقاط صورة لها. ويجب ألا يتعدى عرض خصر الفتاة ورقة الطباعة لتظهر وفقاً لهذا الاختبار مثل عارضات الأزياء. بالإضافة إلى الترويج لصورة سلبية عن النساء، يعرض هذا التحدي العديد من مستخدمي الإنترنت لمرض فقدان الشهية.

## تحدي مومو

تحرش وتهديد وقرصنة وتحرير على الانتحار... يشجع تحدي مومو المشاركين على القيام بأفعال خطيرة تحت التهديد. فقد اخترقت هذه اللعبة تطبيق واتساب وانتشرت في رواق الرسائل حيث يمكن لمستخدمي الإنترنت الاتصال برقم مجهول يجدونه متاحاً في تطبيق ريديت وفيسبوك.







## صندوق الأدوات

### الوقاية قاعدة ذهبية

تتجلى الوقاية أولاً في فتح حوار مع هؤلاء الشباب، هواة أو محترفي ألعاب وتحديات الإنترنت، ومناقشة هذا الموضوع معهم. غالباً ما تكون التحديات عبارة عن لعبة عنيفة، ولهذا يجب تفسير المخاطر التي قد تحملها ألعاب من هذا النوع. وبما أن بعض التحديات قد تقود إلى الموت المحتم، فمن الضروري شرح ذلك الأمر للمراهقين والأطفال.



كما يجب التخلص من هاجس الانتماء إلى مجموعة ما، لأن الشباب الذين يشاركون في هذه التحديات الرقمية الخطيرة مهووسون بهذه الفكرة. كما أنهم يتبعون موجة المنافسة للمشاركة في سباق إلى القمة، دون تراجع أو انهزام وبأي وجه كان.

كيفاش نحيمو الشباب المراهقين من هذه التحديات الرقمية؟



1 التعريف والتحسيس بمخاطر تحدُّ ما خطوة أساسية؛

2 البقاء على علم بأخر التحديات الرقمية؛

3 تتقَدُّ المواقع التي يزورها الطفل عن طريق سجلات محرركات البحث...

4 إخبار الطفل أنه لن يُمنع بالضرورة من استعمال الإنترنت أو شبكات التواصل الاجتماعي إذا اهتم بلعبة ما، فالخوف من الحجز أو العقوبة لا ينبغي أن يشكل عائقاً أمام الحوار.



يتم نشر مئات التحديات يوميا على شبكة الإنترنت. يمكن لتحد ما على شبكة الإنترنت أو مواقع التواصل الاجتماعي أن يكون إيجابيا. مثال: أن تشكر خمسة أشخاص خلال اليوم أو تساعد شخصا من عائلتك أو أن تخبر أباك أو أمك أنك تحبهم.





## الاعتداء الجنسي على الأطفال واستغلالهم في إنتاج المواد الإباحية والتحرش الرقمي

الفصل  
3



يتعرض القاصرون إلى خطر مزدوج في شبكة  
الإنترنت: المواد الإباحية والمتحرشون جنسيا.

وتتكاثر هذه الآفة بسبب تصفح الأطفال للإنترنت باستقلال تام ودون حماية،  
خاصة وأن العديد من المواقع الإباحية تتيح الولوج إلى محتوياتها مجانا ولا تتوفر  
على نظام تحديد الولوج بالنسبة للقاصرين.

أفادت الأرقام الصادرة عن منظمة الأمر المتحدة سنة 2009 أن أزيد من 750.000 متحرش جنسيا يتصل بشبكة  
الإنترنت. كما تشير بعض المعطيات إلى أن طفلا واحدا من بين خمسة أطفال يتعرضون للتحرش الجنسي عبر  
الإنترنت.

### يختبئ المتحرشون جنسيا بيننا على شبكة الإنترنت وراء قناع البراءة واللطافة.





## احذروا ! تعرض الطفل في سن مبكرة للمواد الإباحية

قد يكون له انعكاسات خطيرة على صحته العقلية، بالإضافة إلى اضطرابات جنسية حادة.



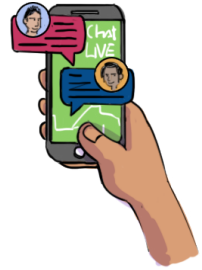
لا يوجد هنالك نموذج محدد لمستغلي الأطفال جنسيا عبر الإنترنت. يمكننا التمييز بين فئتين من مستغلي الأطفال جنسيا على الإنترنت:

- هواة الاستغلال الإباحي للأطفال (المدعوون بالمتلصعين عبر الإنترنت).
- المعتدون جنسيا على الأطفال باستخدام الإنترنت (المدعوون بالمتصيدين عبر الإنترنت).

يتسلل مستغلو الأطفال جنسيا إلى مجموعات داخل مواقع التواصل الاجتماعي فايسبوك وإنستغرام وسناب شات، وكذا إلى مواقع الألعاب الرقمية. ويقومون بعد ذلك بقرصنة الصور الشخصية الخاصة بالقاصرين من مستخدمي الإنترنت وينتحلون شخصياتهم، ثم يقومون بإرساء علاقة ثقة بينهم وبين ضحاياهم قصد التقرب منهم أكثر فأكثر.

### أفادت دراسة المنظمة غير الربحية Action innocence التي يوجد مقرها بسويسرا سنة 2019 ما يلي:

**1** غالبا ما يتم التقرب من الضحايا عبر منصات المحادثات والمنتديات الرقمية الخاصة بالقاصرين. وتعتبر الأسماء الافتراضية والمعلومات الخاصة التي يضعها القاصرون في صفحاتهم (السن والجنس والموقع الجغرافي) أهم ما يثير انتباه مستغلي الأطفال جنسيا؛



**2** تتم المحادثات بعد ذلك بشكل منتظم عبر الرسائل القصيرة الشخصية والمكالمات الهاتفية؛

**3** تتطور علاقة الثقة تدريجيا مع مرور المحادثات؛



**4** يستغل المتحرشون جنسيا عبر شبكة الإنترنت الحساسية العاطفية للأطفال والمراهقين، سواء عبر الإجابة عن أسئلتهم حول المواضيع الجنسية أو من خلال التلاعب بهم نفسيا. وفي بعض الحالات، لا يتردد مستغلو الأطفال جنسيا في محاولة تقديم هدايا لهم أو مكافآت بغرض إغوائهم؛



**5** بعد تعزيز الثقة بينهم وبين هؤلاء الأطفال الذين لا يزالون يفتقرون للتجربة والقدرة على التمييز والحكم، قد يطلب المتحرشون منهم إرسال فيديوهات وصور لهم في وضعية حميمة أو أن يحددوا موعد لقاء مباشر دون علم أولياء أمرهم.



## التحرش عبر الإنترنت: النساء في الواجهة

بنقرة واحدة، نستفيد من تكنولوجيا المعلومات والاتصال

تعتبر الهواتف الذكية والألواح الرقمية والحواسيب والأجهزة الإلكترونية الأخرى الموصولة بالإنترنت في متناول أيدينا. ومع تطور شبكات التواصل الاجتماعي، انتشرت ظاهرة التحرش الرقمي على نطاق أوسع وغير مسبوق في صفوف الصغار سنا.

تقرن العديد من أشكال الاعتداء الرقمي بظاهرة التحرش عبر الإنترنت: انتشار الإشاعات والتحقير وانتحال الشخصية وسرقة البيانات الشخصية والإهانة والسخرية والتنمر عبر الإنترنت، فضلا عن الابتزاز والتحرش الجنسي.

كما تؤثر هذه الظاهرة بشكل مباشر على الصحة العقلية للضحايا ورفاههم، وقد تخلف أضرارا لا يمكن إصلاحها مثل الانتحار والاكتئاب وكذا فقدان احترام الذات.

### النساء أكثر عرضة للتحرش على الإنترنت من رجال بنسب مضاعفة

يوضح التقرير السنوي لجمعية التحدي للمساواة والمواطنة، الصادر سنة 2020، أن فئات النساء الأكثر عرضة للتحرش على الإنترنت في المغرب هن الطالبات بالمدارس الإعدادية والثانوية أو بالجامعات.

يعتبر التحرش من أكثر ممارسات العنف انتشارا على شبكة الإنترنت. التهديد والتشهير وإرسال رسائل إباحية والابتزاز الجنسي، هي أشكال الاعتداء الرقمي التي أكد عليها هذا التقرير. يحتل تطبيق واتساب الصدارة من بين المواقع الاجتماعية التي تنتشر فيها هذه الأفعال، ويليه فيسبوك ثم إنستغرام وماسنجر.

ويلاحظ في معظم أنحاء العالم أن التحرش الرقمي يهدد النساء بشكل مضاعف مقارنة مع الرجال.



## ما يرد في القانون المغربي عن التحرش

تتضمن المادة 503 من القانون الجنائي ما يلي:  
يعاقب بالحبس من سنة إلى سنتين وبالغرامة من خمسة آلاف إلى خمسين ألف درهم، من أجل جريمة التحرش الجنسي، كل من استعمل ضد الغير أوامر أو تهديدات أو وسائل للإكراه أو أية وسيلة أخرى مستغلا السلطة التي تخولها له مهامه، لأغراض ذات طبيعة جنسية.



كما تم تعزيز الإطار القانوني المغربي الخاص بهذه القضايا بالقانون رقم 103.13 المتعلق بمحاربة العنف ضد النساء والصادر بتاريخ 22 فبراير 2018، والذي يفرض عقوبات بخصوص التحرش عبر الإنترنت.  
ورد في الفصل 503-1-1 من هذا القانون ما يلي:

يعتبر مرتكبا لجريمة التحرش الجنسي ويعاقب بالحبس من شهر واحد إلى ستة أشهر وغرامة من 2.000 إلى 10.000 درهم أو ياحدى هاتين العقوبتين كل من أمعن في مضايقة الغير في الحالات التالية:

1. في الفضاءات العمومية أو غيرها، بأفعال أو أقوال أو إشارات ذات طبيعة جنسية أو لأغراض جنسية؛
2. بواسطة رسائل مكتوبة أو هاتفية أو إلكترونية أو تسجيلات أو صور ذات طبيعة جنسية أو لأغراض جنسية.



وقد صادق المغرب على الاتفاقية الدولية حول الجريمة المعلوماتية المعروفة باتفاقية بودابست، والتي دخلت حيز التنفيذ منذ فاتح أكتوبر سنة 2018. وتتيح المصادقة على هذه الاتفاقية للسلطات القضائية المغربية إمكانية متابعة مرتكبي الجرائم المعلوماتية العابرة للحدود، خاصة منهم المتحرشون عبر الإنترنت.



## صندوق الأدوات

# كيف نحمي الأطفال من المتحرشين على شبكة الإنترنت

### 1 الرقابة الأبوية

بلاني تكبر الشاشة...  
غادي نقلب في سجل  
تصفح الانترنت



توجد مجموعة من الوسائل الرقمية للرقابة الأبوية والتي تساعد على الحد من مخاطر تعرض الأطفال للصور الإباحية. ويمكن تحميل تطبيقات في أجهزة الأطفال وأولياء أمرهم الموصولة بالإنترنت أو وضع برامج للتعرف على المحتويات غير اللائقة ومنع الدخول إلى المواقع الإباحية. من واجب الآباء تشغيل هذه التطبيقات وضبطها من أجل حمايتها من التعطيل أو استخدامها بواسطة كلمة السر.

تساعد هذه الوسائل على حجب مواد أخرى غير مناسبة للأطفال والقاصرين (مثلا المحتويات العنيفة ومواقع لعب القمار، إلخ)، وكذا تحديد المدة الزمنية القصوى لاستخدام جهاز إلكتروني ما وتوقيت الاتصال بالإنترنت.

فين نلقا هاد الأدوات باش نحمي  
راسي ونحمي ولادي؟



تتضمن شبكة الإنترنت العديد من العروض الخاصة بالرقابة الوالدية، حيث تكون مجانية أو مؤدى عنها. وتتجلى أسهل طريقة في استخدام الوسائل التي توفرها شركة الجوال أو الإنترنت التي تشتركون معها، أو اللجوء إلى الأدوات المدمجة في نظام التشغيل الخاص بالجهاز الذي يستعمله طفلكم.



## بعض الأدوات المتاحة مجاناً لأولياء الأمر

### الحاسوب

الرقابة الوالدية في نظام Mac OS  
[/https://www.apple.com/fr/families](https://www.apple.com/fr/families)  
الرقابة الوالدية في نظام Windows  
<https://account.microsoft.com/family/about>



### الهاتف الذكي

iPhone: الوقت المستغرق أمام الشاشة  
[/https://www.apple.com/fr/families](https://www.apple.com/fr/families)  
Android : «Family Link» أداة غوغل للرقابة الوالدية  
[/https://families.google.com/intl/fr/familylink](https://families.google.com/intl/fr/familylink)



### اللوحة الرقمي

iPad: الوقت المستغرق أمام الشاشة  
[/https://www.apple.com/fr/families](https://www.apple.com/fr/families)  
Android : «Family Link» أداة غوغل للرقابة الوالدية  
[/https://families.google.com/intl/fr/familylink](https://families.google.com/intl/fr/familylink)



\*تجدر الإشارة إلى أن هذا الدليل يقترح حلولاً توجيهية فقط، حيث أن بعضها منها قد يكون خاضعاً لشروط معينة.



لا يوفر مقدمو خدمات شبكة الإنترنت تطبيقا على الإنترنت بل يقدمون إرشادات ونصائح.

## شركة اتصالات المغرب



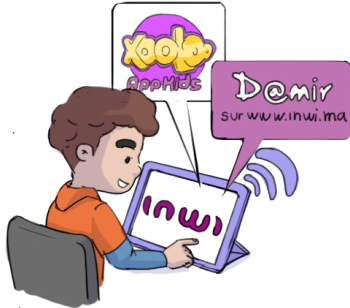
تقدم شركة اتصالات المغرب خدمة (مؤدى عنها) للرقابة الوالدية تدعى **Kaspersky Safekids**. يتيح هذا التطبيق مجموعة من الوظائف: تدبير وقت النظر إلى الشاشة والتحكم في المدة الزمنية المستغرقة في مواقع التواصل الاجتماعي وحجب المحتويات وتتبع الموقع الجغرافي، إلخ.

**Norton Family**: خدمة مجانية للرقابة الوالدية توفرها شركة اتصالات المغرب لزيائنها، حيث تمكن الوالدين من تتبع استخدام طفلهم لشبكة الإنترنت وتأمينه.

كما تتيح لهم إمكانية الإشراف على أنشطة أبنائهم الرقمية و/أو منعهم منها، بالإضافة إلى إشعار تلقائي يصل عبر البريد الإلكتروني لأولياء الأمر كلما تجاهل أبنائهم إنذارا ما وحاولوا زيارة مواقع غير لائقة.

**Smart Kids**: خدمة تساعد الآباء وأولياء الأمر على تحديد موقع أبنائهم في أي وقت بواسطة إشارة رقمية.

## شركة INWI



**Damir** تطبيق ترفيهي وتعليمي متوفر في خانة «فضاء الأطفال» على موقع شركة INWI. يبدو هذا التطبيق دائما مشغول، إلا أن زائر الموقع يجب أن يكون زبونا للشركة إن أراد استخدامه عبر متجر التطبيقات الخاص بهاتفه الذي.

كما تعقد شركة INWI علاقات شراكة مع منظمة الأمم المتحدة للطفولة (حملات تحسيس الوالدين والأطفال والمدرسين). وتوفر INWI كذلك أدوات خاصة بالرقابة الوالدية مثل تطبيق

**Xooloo App Kids**



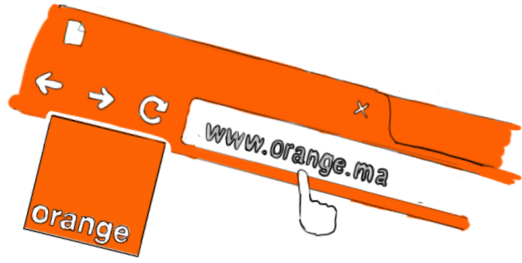


## ORANGE شركة

يتضمن موقع Orange.ma صفحة مخصصة لتحسيس الشباب والأطفال بالاستخدام المسؤول للإنترنت:

<https://corporate.orange.ma/Bien-Vivre-Le-Digital/Usage-responsable/Usage-responsable/Votreenfant-joue-aux-jeux-video-que-savoir>

تقترح شركة Orange عبر شعار "التعايش الأمثل مع الفضاء الرقمي" أنشطة تحسيسية لفائدة التلاميذ وورشات مجانية لإطلاع الشباب على تقنيات التشفير المعلوماتي. كما تقدم دليلا حول الاستعمالات الإيجابية للشاشات.



\*تجدر الإشارة إلى أن هذا الدليل يقترح حلولاً توجيهية فقط، حيث أن بعضها منها قد يكون خاضعاً لشروط معينة.



## 2 الحوار

صحيح أن أداة الرقابة الأبوية تقلل من مخاطر تعرض أطفالكم للصور الإباحية، لكنها لا تضمن حمايتهم بشكل كلي. ولهذا السبب، من الضروري التذاور معهم وعدم إلقاء الذنب عليهم لمجرد تعرضهم بشكل لا إرادي لصور صادمة. لا يتجرأ الأطفال في بعض الأحيان على التحدث عما رأوه خوفاً من العقاب و/أو الحرمان من الشاشات. يجب أخذ أبعاد هذا الإحراج -«حشومة»- بعين الاعتبار وكسب ثقة طفلكم ليحكى لكم ما يجري.





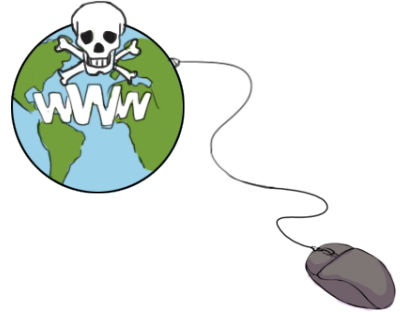
## وأخيرا

### البرنامج العالمي لمحاربة جميع أشكال الاعتداء على الأطفال



مكّن برنامج **Child Protection System CPS** الذي استخدم في 50 ولاية أمريكية و96 بلداً، من إيقاف 12 488 متحرشاً وإبطال أزيد من 600 000 حالة إساءة للأطفال. لكن هذا المعدل الأخير لا يزال ضعيفاً أمام حالات الاستغلال التي تم الإبلاغ عنها، مما جعل المنظمة غير الربحية الواردة أعلاه تلتزم بالتعاون مع منصات وسائل التواصل الاجتماعي من أجل تحسين فعالية هذه الأداة. وتجدر الإشارة إلى أن هذا البرنامج يواجه مشاكلًا متنامية فيما يتعلق بحماية سرية البيانات، مما يعيق تطوره. كما أن هذه الأداة تُستخدم من طرف 12 000 محقق عبر العالم.

تتيح مواقع الاستغلال الإباحي للأطفال إمكانية مشاركة وتحميل ومشاهدة المحتويات مجاناً. فهي تشبه المواقع التي يستعملها مستخدمو الإنترنت لتحميل الأفلام أو البرامج بشكل غير قانوني. ويعتقد الأشخاص الذين يدخلون هذه المواقع أن هويتهم محجوبة، إلا أن الأمر ليس كذلك على الإطلاق.



يُظهر برنامج **CPS** على خريطة موقع وعنوان (IP) الحواسيب التي استخدمت المنصات المراقبة من طرف هذا البرنامج لتحميل صور أو فيديوهات تم الإبلاغ عنها أو صادرتها الشرطة. تشمل هذه الأداة التكنولوجية قاعدة بيانات يتم تحيينها بانتظام وتتوفر على 18.5 مليار تسجيل. ويقوم البرنامج بعد ذلك بفرز الحالات التي تم رصدتها قبل التركيز على المتحرشين الأكثر بروزاً على الإنترنت، والذين يعتبرون الأكثر خطورة.



## المعطيات الشخصية : ما السبيل لحمايتها؟

الفصل 4

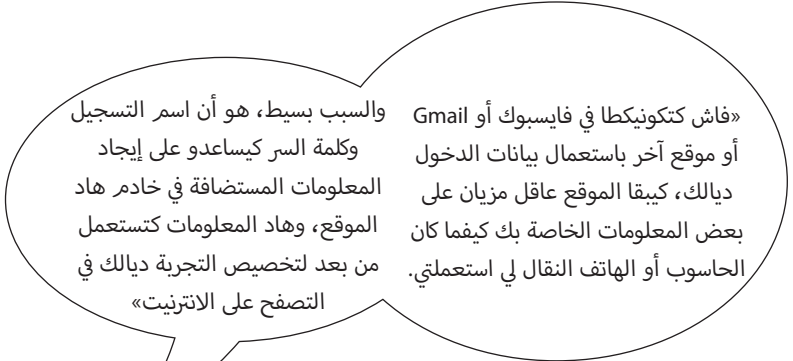


تقع «المعطيات ذات الطبيعة الشخصية» في قلب كل الاهتمامات. وتفرض علينا شبكة الإنترنت الاستمرار في مشاركة هذا النوع من المعطيات. فبمجرد الاشتراك في موقع ما أو الانخراط في شبكة اجتماعية أو لعبة الكترونية جماعية، نشارك مجموعة من المعطيات ذات الطبيعة الشخصية والتي تنتقل لاحقا من شركة لأخرى.

ولتجنب مشاركة معطياتنا الشخصية، صدرت قوانين لحماية هذه البيانات.

### ماذا نقصد بالمعطي الشخصي؟

اسم أو صورة أو بصمة أو عنوان البريد أو عنوان الكرتوني أو رقم الهاتف أو رقم الضمان الاجتماعي أو رقم تسجيل أو عنوان IP أو بيانات تسجيل الدخول أو تسجيل صوتي، إلخ. عندما نقوم بزيارة موقع ما لأول مرة، غالبا ما نُطلب منا بعض المعلومات، حيث تمكن هذه المعطيات من تخصيص التصفح داخل هذا الموقع.

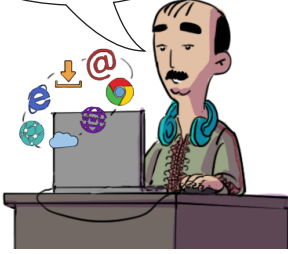


والسبب بسيط، هو أن اسم التسجيل وكلمة السر يساعدو على إيجاد المعلومات المستضافة في خادم هاد الموقع، وهاد المعلومات كتستعمل من بعد لتخصيص التجربة ديالك في التصفح على الانترنت»

«فاش كتكونيكطا في فيسبوك أو Gmail أو موقع آخر باستعمال بيانات الدخول ديالك، كيبقا الموقع عاقل مزيان على بعض المعلومات الخاصة بك كيفما كان الحاسوب أو الهاتف النقال لي استعمالتي.



لحد الآن، مكانين حتا شي مشكل  
فبرنامج التصفح...غير كون هاني!



## هل يجب قبول ملفات تعريف الارتباط (Cookies) ؟

انتبهوا! يؤكد القانون رقم 08-09 أنه يجب على الموقع الذي يستخدم ملفات تعريف الارتباط المتعلقة بالمعطيات الشخصية أن يحصل على موافقة المتصفح قبل وضع هذه الملفات. كما ينبغي أن يحدد الغاية من استعمال هذه الملفات وأن يوضح للمتصفح كيفية الاعتراض عليها.

منذ بدايات الويب، لا يمكن قراءة ملفات تعريف الارتباط إلا من طرف المواقع التي تضعها. ولا يمكن إلا للموقع الذي يقوم بتخزين هذه المعلومة استعمالها لاحقا ما دامت سارية المفعول.

## أسئلة وأجوبة للمزيد من الفهم

هل تتسبب ملفات تعريف الارتباط حقا في مشكل ما على مستوى سرية البيانات؟ لماذا يفرض القانون المذكور أعلاه على جميع ناشري المواقع الالكترونية أن يطلبوا بشكل صريح موافقة مستخدم الانترنت فور دخوله للموقع؟ إذا قمتم باستخدام متصفح الويب Chrome مثلا، يمكنكم رؤية كل ملفات الارتباط الخاصة بكم ومجالات تخزينها من خلال النقر على الزر F12 ثم على «موارد» وبعد ذلك «ملفات تعريف الارتباط».



يعني إذا وضعت cookie وأنا كنقوم  
بحجز تذكرة قطار مثلا فموقع oncf.ma  
ومن بعد دخلت لموقع آخر، مغاديش  
يقدر هاد الموقع الثاني يقرأ cookie لي  
هدرنا عليه أو يعرف تواريخ السفر ديالي





شنو غادي يوقع  
إلا بركت على «لا»؟



## هل يمكننا رفض ملفات تعريف الارتباط؟

تضع شركات الإعلانات ملفات تعريف الارتباط لتتبع نشاطكم على الانترنت: فعندما تدخلون لموقع توجد به إعلانات، تضع Google ملف الارتباط أو تقوم بتعيينه، ثم تخزن فيه المعلومات المتعلقة بالصفحة التي قمتم بزيارتها.

تتلقون بعد ذلك إعلانات موجهة لها صلة بالأبحاث التي قمتم بها، حيث تتجلى وظيفة هذه الملفات في إعادة توجيه الإعلانات.

مفهوم إعادة التوجيه أو «إعادة الاستهداف» هو الذي يعطينا الانطباع بأننا مراقبون في جميع تحركاتنا على شبكة الانترنت.

مصدر PXAgency : [https://pxagency.fr/cookies-internet-accepter/?utm\\_source=cpp](https://pxagency.fr/cookies-internet-accepter/?utm_source=cpp)

وكدوز أيام حتى كتلقا في موقع  
آخر ما عندوش أدنى علاقة  
بالتجارة إشهار ديال نفس  
المنتجات لي كنتي شفتي قبل

كتقوم بزيارة مواقع التسوق  
وكتشوف منتجات بلا ما توضعها  
بالضرورة في سلة المشتريات





## سيطرة ملفات الارتباط وموافقة المتصفحين، ابقوا على علم بحقوقكم!

تعتبر شروط وأحكام الاستخدام، التي تكون غالبا طويلة ومفصلة ولا يعيرها المتصفحون اهتماما كبيرا، أول نافذة تطل على بياناتكم الشخصية.

ولهذا، فمسألة الموافقة تُطرح بشكل مُلحّ عندما يكون تصفح موقع ما مقترن بقبول ملفات الارتباط ووثيقة شروط الاستعمال، التي تكون أحيانا معقدة وصعبة الفهم.

## ما موقف المغرب من هذا الموضوع؟

في المغرب، يُحدّد إطار استخدام ملفات الارتباط بالخطوط التوجيهية المتعلقة بملاءمة المواقع الإلكترونية لمقتضيات القانون رقم 09-08:

«يتعين على الموقع الإلكتروني، الذي يستعمل ملفات الربط تتعلق بمعطيات شخصية، أن يحصل على رضا المتصفح قبل القيام بوضعها. كما يتعين عليه كذلك أن يحدد الغاية من استعمال هذه الملفات وأن يوضح للمتصفح الوسائل الكفيلة بالتعرض عليها.»



يوضح النظام العام لحماية البيانات (RGPD)، الذي دخل حيز التنفيذ منذ 25 ماي 2018، ما يلي:  
"إن ربط توفير خدمة ما بجمع معطيات ثانوية بالنسبة لهذه الخدمة يشكل عائقا أمام الحصول على موافقة حرة. ولهذا، لا يجب منع تصفح موقع ما في حال رفض المتصفح وضع ملفات الربط."  
(ترجمة لنص القانون - غير متوفر باللغة الأصلية)

لمزيد من المعلومات حول هذا الموضوع، يمكنكم الاطلاع على منشورات اللجنة الوطنية لحماية المعطيات ذات الطابع الشخصي:

<https://www.cndp.ma/images/documents/BD-CNDP-fr.pdf>  
<https://www.cndp.ma/images/documents/CNDP-guide-conformite-sites-web-fr.pdf>



## الممارسات الفضلى من أجل تدبير فعال لمعطياتكم الشخصية



### صندوق الأدوات



تعتبر حماية الحياة الخاصة والمعطيات الشخصية بمثابة صراع فردي مع فضاء رقمي صُنِع بواسطة الجمع والتخزين الهائل للبيانات لأغراض تجارية وتسويقية.

ينبغي على مستخدم الانترنت الوعي منذ النقرات الأولى بأهمية الأرشفة المعلوماتية.

فعند كل استخدام للإنترنت، يتم تخزين آثار التصفح وملفات الربط وكذا البيانات الوصفية للسلوك الرقمي للمتصفح، حيث يمكن استخدام هذه الأخيرة لأغراض الاستهداف الإعلاني.

### هذه بعض الممارسات المُثلى التي ينبغي اعتمادها دون تحفظ لحماية المعطيات الشخصية:

**1** إلغاء التطبيقات والبرامج غير الضرورية من الهاتف الذكي والحاسوب؛

**2** تعطيل بيانات تحديد المواقع وإعادة ضبط الأذن الممنوحة للخدمات؛

**3** إعادة ضبط معرف الإعلانات؛

**4** استخدام تقنية تشفير المحتوى على الهاتف الذكي أو الحاسوب؛

**5** استخدام الشبكة الافتراضية VPN الخاصة والمؤمنة (وهو برنامج من شأنه خلق قناة مؤمنة بين المستخدم وشبكة الانترنت)؛

**6** ضبط برنامج الحماية لمنع الاستخدامات غير المرغوب فيها؛

**7** استخدام برنامج تصفح الانترنت ومحرك بحث يحترمان الحياة الخاصة.







## توجد هنالك مجموعة من الآليات والبرامج التي تحترم سرية البيانات الشخصية.

يقترح هذا الدليل بعض النماذج التوجيهية للوسائل المتاحة مجانا من أجل حماية معطياتكم الشخصية بشكل أفضل\*.



موقع **Panopticlick** يمكن من اختبار حماية متصفح الإنترنت الخاص بك ضد تتبع المواقع لنشاطك والاطلاع على حجم علامة الأصابع التي يتركها هذا المتصفح في كل موقع تزوره.



المتصفح **Brave** هو مانع للإعلانات والمتعقبين على الإنترنت. كما أنه برنامج يمكن أي ناشر للمحتوى على الإنترنت من ربح المال بواسطة الإعلانات التي تكون ملائمة.



**KeePass**

**KeePass** وسيلة مصدرها مفتوح ومجاني، تمكن من تخزين كلمات السر داخل قاعدة بيانات وحيدة ومغلقة بواسطة مفتاح رئيسي أو ملف مفتاح.



**Signal**

**Signal** بديل حقيقي لتطبيق واتساب وبرنامج شهير يتم تمويله بالتبرعات ويستعمل تقنية التشفير بين الطرفين (Chiffrement de bout en bout).



**Privacy Badger**

**Privacy badger** هو امتداد لمتصفح الانترنت، يمنع متعقبى الإعلانات من المراقبة السرية لنشاطكم الرقمي. إذا قام متعقب إعلاني بتتبع نشاطكم على العديد من صفحات الويب دون إذتكم، سوف يمنع تلقائيا من نشر أي محتوى لكم.

\* تجدر الإشارة إلى أن هذه البرامج الحاسوبية قد تشهد تغييرا في نمط الولوج أو يصبح استعمالها مهملا.



## الفصل 5

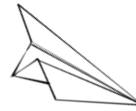
### 5 نصائح للتدقيق في المعلومات

خاصنا دائما نتحققو من المعلومة. هادو  
5 نصائح باش تتأكد من مدى مصداقية  
مصادر الخبر



#### 1 تحديد هوية ناشر الخبر

من صاحب الخبر؟ هل يتعلق الأمر بوسيلة إعلام معروفة أو شخصية عمومية؟ أم هو موقع الكتروني مجهول أو شخص ما على الانترنت لم تسمعو عنه من قبل؟  
في حالة الشك، يجب دائما الاطلاع على المصادر الموثوقة والمعترف بها.



#### 2 اعتماد المبدأ التالي: إذا كان مصدر خبر ما على الانترنت مجهولا فهو خبر خاطئ بلا شك؛

يُنصح دائما اللجوء إلى المنابر الإعلامية المعترف بها والصحفيين والخبراء المعروفة هويتهم. لكن انتبهوا، فهذا لا يعني أنها تنقل بالضرورة أخبارا مؤكدة.





### 3 مقارنة وتنظيم المعلومات بعد تحديد مصدر الخبر

إذا نقلت مجموعة من وسائل الإعلام الخبر نفسه مع الإشارة إلى مصادر مختلفة، فإن الخبر حتماً مؤكد. وعلى عكس ذلك، يجب توخي الحذر الشديد أمام خبر دون مصدر ولا وجود له في أي موقع على الإنترنت.



### 4 الرجوع قدر الإمكان إلى المصدر الرئيسي

لا تشير العديد من الأخبار المتواجدة في مواقع التواصل الاجتماعي إلى مصدر المعلومة. ولهذا فمن الأفضل تلقي الخبر مباشرة من محادثة ما بدلا من الوثوق بأقوال شخص تحدث مع الشخص الذي حضر المحادثة. يجب اجتناب المصادر غير المباشرة مثل "زوج صديقة زميل في العمل" أو "صديق صديق لي". كما ينبغي تفادي نوع من المصادر يُزعم أنها مؤسسية لكنها غير واضحة مثل "شخص يشتغل مع الشرطة/ مع المديرية العامة للأمن الوطني/ في الجيش..".

### 5 علينا دائما أن نُفَنِّع أنفسنا بأن الخبر كلما كان مفاجئا وغير متوقع، كلما وجب التدقيق فيه وتفصيله

احذروا كذلك من الأدلة الكاذبة والعبارات مثل "الكل يعلم أن..". أو "لا داعي لأن تثبت أن..".



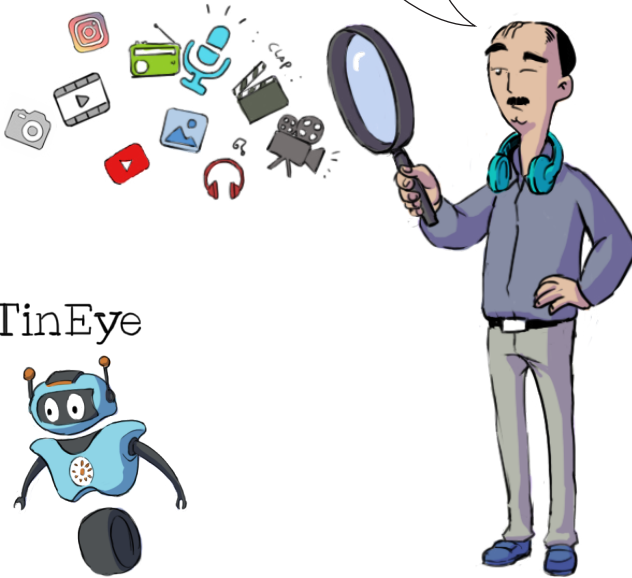


## كيف تقوم بتدقيق المعلومات بمفردك ؟



### صندوق الأدوات

كنتنشر صور وفيديوهات فالهواتف الذكية  
كاتضرب على الشُّعاع. المشكل هو أننا خاصنا  
دائما نتأكدو من صحتها.

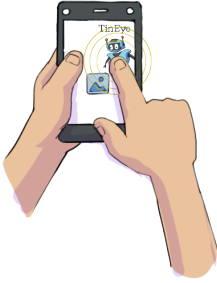
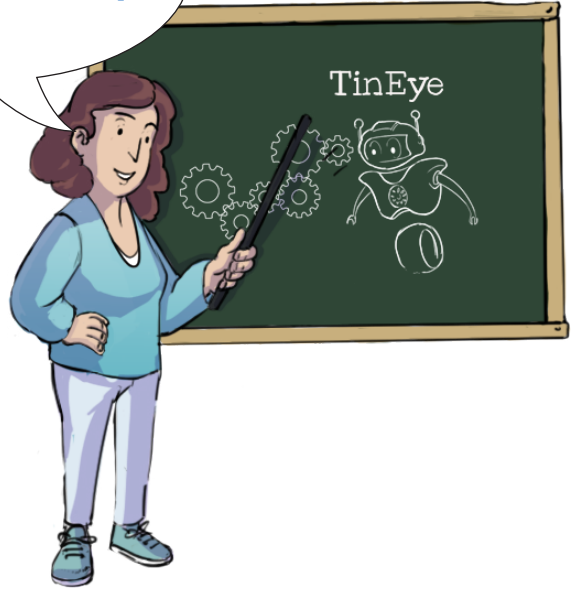


### كيف تتأكد من صحة الصور في الهاتف الذي ؟

**TinEye** : أداة مجانية للبحث عن الصور العكسية وبمثابة محرك للحصول على الصور والعثور على مكان ظهورها على الإنترنت. تساعدك هذه الوسيلة على إيجاد الصورة المراد العثور عليها أو صورة مماثلة ظهرت في أماكن أخرى على الإنترنت.



## TinEye إرشادات الاستعمال



**1** كل ما عليك فعله هو الدخول للموقع وتسجيل أو تحميل الصورة المراد البحث عنها من خلال النقر فوق رمز السهم الموجود أمام مربع البحث لتسجيل الصورة أو وضع عنوان رابط الويب الخاص بها في خانة البحث ثم النقر على أيقونة البحث؛

**2** ادخل لموقع <https://tineye.com> عبر برنامج التصفح الخاص بهاتفك، ثم انقر "تحميل الصورة" وابحث عن نسخة الصورة المسجلة في الوثائق أو رواق الصور الخاص بالهاتف أو ضع عنوان رابط الويب الخاص بها في خانة البحث TinEye؛



**3** اختر صورة من الصور المحصل عليها ثم قم بالتحويل بين "صورتك" و "الصورة المطابقة".

\*تجدر الإشارة إلى أن هذا الدليل يقترح حلولاً توجيهية فقط، حيث أن بعضاً منها قد يكون خاضعاً لشروط معينة.



## غادي نقلب على الصورة العكسية في غوغل



يمنح **Google image** برنامجا للبحث عن الصور العكسية، حيث يحدد تاريخ استعمال الصورة لأول مرة ومكان وزمن الحدث الذي تمثله. كما يساعد على التحقق من أن مصدر الصورة موثوق.

**1** قم بتسجيل أو تحميل الصورة المراد البحث عنها، أو كذلك وضع رابط الويب الخاص بها. احرص على وضع رابط URL الخاص بالصورة الحقيقية، وليس رابط الصفحة بأكملها؛

فينهاية أيقونة الكاميرا؟

**2** ادخل للموقع <https://images.google.com>؛

**3** ادخل لقائمة المحتويات عبر برنامج التصفح ومرر الزر إلى الأسفل ثم اختر «اطلب موقع المكتب». في بوابة Google Chrome، ستجد قائمة المحتويات بالنقر على الثلاثة نقاط الموجودة في الأعلى على يمين الشاشة. وفي برنامج التصفح iOS Safari، توجد القائمة في الوسط أسفل الشاشة؛



**4** انقر فوق أيقونة الكاميرا الموجودة في خانة البحث؛

**5** لديك خياران: إما أن تضع رابط الصورة المراد البحث عنها في خانة البحث، أم تختار "تحميل صورة" لتحميلها انطلاقا من المكان الذي تم فيه تسجيلها على الهاتف؛



تأكد من النتائج لمعرفة مكان وزمن استعمال الصورة؛  
إذا عدت بالبحث بعيدا إلى الوراء، ستجد مكان استعمال الصورة لأول مرة ومالك حقوق الطبع والنشر للصورة.



## كيف نكشف الفيديوهات الكاذبة أو الخارجة عن السياق والمنشورة بتقنية "التزييف العميق"؟

يمكن صنع فيديوهات من لا شيء أو التلاعب بها ببراعة تامة قصد تضليل المشاهدين. كما يمكن الاعتماد على التكنولوجيا الحديثة لفبركة هذه الفيديوهات.



**Youtube DataViewer** : تطبيق رقمي وضعته منظمة العفو الدولية للتحقق من مصدر فيديو ما على اليوتيوب.



**Kapwing** : تطبيق مجاني للتحقق مما إذا تم التلاعب بسرعة قراءة الفيديو.

لتصفح دليل استخدام هذا التطبيق، يمكنك زيارة الموقع التالي:

[/https://www.kapwing.com](https://www.kapwing.com)

\*تجدر الإشارة إلى أن هذا الدليل يقترح حلولاً توجيهية فقط، حيث أن بعضها منها قد يكون خاضعاً لشروط معينة.



## توصيات



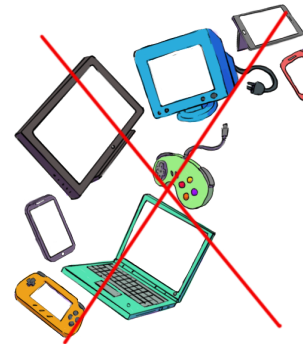
تحتل شبكة الإنترنت حيزا هاما في الحياة اليومية للأغلبية العظمى من الشعب المغربي. فقد تضاعف استخدام الإنترنت بشكل كبير ومتسارع في ظل الأزمة الصحية الناجمة عن وباء كورونا المستجد وما خلفته من تحولات في أنماط عيشنا. تهيمن الصور والأصوات والكلمات على أنشطتنا اليومية وتساهم في تنمية التربية المدنية والتربية على المواطنة فينا وتطوير معارفنا وتعزيز انفتاحنا على العالم. ولترجمة معنى ومغزى هذه الرسائل، لا بد من تلقين صغار الشباب والكبار، على حد سواء، كيفية التحقق من صحتها.

وكما أشرنا في المقدمة، لا يسعى هذا الدليل بتاتا إلى تشويه صورة الإنترنت، بل بالأحرى إلى مُصالحتنا مع هذه الوسيلة التواصلية والإعلامية، حتى منا الأكثر اعتراضا على ذلك. كما يهدف إلى تمكين الأغلبية من استعمالها في اطمئنان تام، وذلك بواسطة أدوات وآليات تساعدنا على تصفح الإنترنت في كامل المسؤولية ومصاحبة صغار الشباب ومستخدمي الإنترنت الأكثر عرضة للخطر داخل هذا الفضاء الرقمي.

وبعيدا عن دافع التحذير، يتمحور هذا الدليل حول توصيات يجب إعمالها لضمان تصفح آمن ومسؤول للإنترنت، إذ يمكن تلخيصها كالآتي:

### بخصوص تعرض الأطفال للشاشات، ينصح ما يلي:

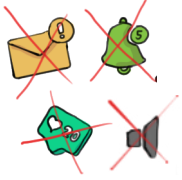
- عدم الجلوس أمام الشاشات إطلاقا بالنسبة للأطفال دون العامين؛
- عدم قضاء الأطفال الذين يتجاوز عمرهم العامين أكثر من ساعة واحدة يوميا في مشاهدة التلفزيون أو الفيديوهات أو ممارسة ألعاب الحاسوب. تفيد الإرشادات الجديدة التي أصدرتها منظمة الصحة العالمية سنة 2019 بشأن صحة الأطفال الصغار أن حظر الشاشات كليا يكون في سن العامين، حتى أن البعض يفضل منعها بشكل نهائي قبل سن الثالثة؛
- ينصح تعود الأطفال على قراءة القصص وممارسة الأنشطة البدنية؛
- الرقابة الأبوية لمدة استعمال الأطفال للإنترنت وطبيعة اتصالهم الرقمي ضرورة ملحة لضمان استخدام صحي وآمن للشاشات؛
- إضافة إلى تأثير الشاشات على القدرات الذهنية للأطفال الصغار، يشكل التعرض المفرط لها خطرا كبيرا على كل من الأطفال والكبار. ولذلك ينبغي تحديد وقت النظر إلى الشاشة بالنسبة لجميع الفئات العمرية؛







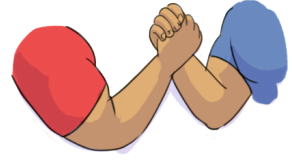
## حماية الأطفال من الإدمان الرقمي، يجب الالتزام بما يلي:



- قدوة الوالدين شرط أساسي؛
- تعطيل الإخطارات للتقليل من الرغبة الملحة في تصفح الهاتف فور تلقي إشارة إنذار؛
- خلق فضاءات خالية من الشاشات في البيت لتقليص وقت النظر إلى الشاشة.

## توصيات بخصوص الوقاية من مخاطر التحديات الرقمية:

- الحرص على أن يكون طفلكم قد بلغ السن المناسب أو النضج الكافي للانخراط في مواقع التواصل الاجتماعي؛
- إخبار من حولكم عن مخاطر تحد ما خطوة هامة؛
- تتبع سجلات التصفح التي يزورها الطفل أو الشاب.



## توصيات بخصوص التدقيق في الحقائق:

- تحديد هوية ناشر الخبر؛
- اعتماد المبدأ التالي: إذا كان مصدر خبر ما على الانترنت مجهولا فهو خبر خاطئ بلا شك؛
- مقارنة وتنظيم المعلومات بعد تحديد مصدر الخبر، وذلك من خلال الاطلاع على المصادر الرسمية للأخبار (وكالات الأنباء والصحف الإخبارية) للتأكد من تداول منابر إعلامية أخرى هذا الخبر؛
- الرجوع قدر الإمكان إلى المصدر الرئيسي؛
- اعتماد المحركات والأدوات المتنوعة والمتجددة التي تساعد على التأكد من الخبر (خانة التدقيق في الحقائق بموقع Médias24، Africa Check، Les décodeurs، خانة الكشف عن الأخبار الزائفة بموقع Ledesk.ma)؛
- علينا دائما أن نُقنع أنفسنا بأن الخبر كلما كان مفاجئا وغير متوقع، كلما وجب التدقيق فيه وتفصيله.





## توصيات لحماية أطفالكم من المتحرشين على شبكة الإنترنت:

إضافة إلى الرقابة الأبوية، من الضروري التواصل بشكل دائم مع أطفالكم وعدم إدانتهم والإصغاء إليهم ليثقوا بكم ويحكو لكم عن تجاربهم مع المحتويات غير اللائقة. نجد من بين الأدوات الخاصة بحماية الأطفال من هذه المحتويات برنامج (Child Protection System (CPS)، وهو برنامج عالمي لمحاربة شتى أشكال الاعتداء على الأطفال.

## توصيات لحماية معطياتكم الشخصية:

يعد استخدام جميع المعلومات التي يتم نشرها على يوتيوب أو فيسبوك أو أي منصة أخرى. وتفسر شروط الخدمة الخاصة بالمواقع التي تتم زيارتها كيفية إعادة استعمال معطياتنا. ولذلك فمن اللازم أخذ هذا الأمر بعين الاعتبار.

كما أن استخدام الصور التجسدية (الأفاتار) والأسماء المستعارة يساهم في تعزيز حماية الحياة الخاصة. فقبل نشر خبر ما، من الضروري التأكد من أنه لا يمس بسمعتم أو سمعة الآخرين ولا يمثل خرقا للقانون. وينبغي التحقق من صحة أي خبر تم نشره. يوجد هنالك إطار مرجعي دولي لحماية البيانات.







## قائمة المحتويات

- 04 صفحة ————— معجم ●
- 07 صفحة ————— مقدمة ●
- 08 صفحة ————— الجزء الأول: الاتصال المفرط بالإنترنت والإدمان على الشبكة الرقمية ●
- 16 صفحة ————— الجزء الثاني: التحديات الرقمية التي تستهدف الشباب ●
- 20 صفحة ————— الجزء الثالث: الاعتداء الجنسي على الأطفال واستغلالهم في إنتاج المواد الإباحية والتحرش على الإنترنت ●
- 30 صفحة ————— الجزء الرابع: المعطيات الشخصية: ما السبيل لحمايتها؟ ●
- 36 صفحة ————— الجزء الخامس: 5 نصائح للتدقيق في المعلومات ●
- 42 صفحة ————— توصيات ●



## طاقم التحرير و الإعداد

**رئاسة التحرير:** نرجس الرغاي، رئيسة مجموعة العمل وعضوة بالمجلس الأعلى للاتصال السمعي البصري؛

**تحرير النسخة الأصلية:** لطيفة الطايح الورطاسي ومحمد أمين بوعزاوي، المديرية العامة للاتصال السمعي البصري؛

**تصميم الرسومات الحاسوبية:** حمزة طموح، المديرية العامة للاتصال السمعي البصري؛

**الترجمة:** أميمة الخطابي، كتابة مجموعة العمل الخاصة بموضوع «التقنين ووسائل الإعلام الرقمية».

الهيئة العليا للاتصال السمعي البصري  
جميع الحقوق محفوظة © 2021

## للاتصال بنا

البريد الإلكتروني : [info@haca.ma](mailto:info@haca.ma)

الهاتف: +212 5 37 57 96 00

الفاكس: +212 5 37 71 42 74

زوروا موقعنا: [www.haca.ma](http://www.haca.ma)

الهيئة العليا للاتصال السمعي البصري، فضاء النخيل،  
قطعة 26 ، زاوية شارع النخيل والمهدي ببنركة،  
ص.ب: 20590، حي الرياض الرباط





الهيئة العليا للاتصال السمعي البصري  
ⵛⵓⵍⵏⵓⵎ ⵛⵓⵎⵎⵓⵏⵉ ⵛⵓⵎⵎⵓⵏⵉ ⵛⵓⵎⵎⵓⵏⵉ  
Haute Autorité de la Communication Audiovisuelle

[www.haca.ma](http://www.haca.ma)