Directrizes relativas à Protecção de Dados Pessoais para África

Uma iniciativa conjunta da Internet Society
e Comissão da União Africana

9 de Maio de 2018

Internet Society

African Union

Introdução

Em 2014, os membros da União Africana (UA) aprovaram a Convenção da União Africana sobre Cibersegurança e Protecção dos Dados Pessoais ("a Convenção")[1]. Os Ministros da UA responsáveis pela Comunicação e Informação e Tecnologia da Comunicação (CICT) e Serviços Postais confirmaram o seu empenho na Convenção no Comité Técnico Especializado da União Africana sobre Comunicação e na Declaração Ministerial de TIC (AU/CCICT-2)[2].

A Declaração estabeleceu um forte objectivo de acção africana sobre a cibersegurança e protecção dos dados pessoais para o benefício de África. Em particular, convidou a Comissão da União Africana (CUA) a desenvolver as directrizes sobre a proteção de dados pessoais (Parág. 31).

Para facilitar a implementação da Convenção, a CUA pediu à Internet Society (ISOC) para desenvolver em conjunto as Directrizes da Proteção da Privacidade e dos Dados Pessoais para África ("as Directrizes"). As Directrizes foram criadas com contributos de peritos em privacidade regionais e globais, incluindo especialistas em privacidade da indústria, académicos e grupos da sociedade civil.

As Directrizes realçam a importância de assegurar a confiança nos serviços em linha, como factor chave para manter uma economia digital produtiva e benéfica. Também incluem informação sobre como ajudar os indivíduos a ter um papel mais activo na protecção dos seus dados pessoais, enquanto reconhece que, em muitas áreas, os resultados positivos para os indivíduos dependem da acção positiva de outras partes interessadas.

As Directrizes estabelecem 8 recomendações, agrupadas sob três títulos:

- Dois princípios fundamentais para criar confiança, privacidade e uso responsável dos dados pessoais;
- Oito recomendações para acção das seguintes partes interessadas:
    - Governos e responsáveis políticos;
    - Autoridades da Protecção de Dados (DPA);
    - Controladores de dados e processadores de dados;
- Oito recomendações sobre os seguintes temas:
    - Soluções de várias partes interessadas;
    - Bem-estar do cidadão digital;
    - Medidas de habilitação e apoio.

A privacidade e protecção dos dados pessoais é um domínio amplo e sempre em mudança; as Directrizes não se encontram finalizadas, são um ponto de partida de um processo em evolução de política em desenvolvimento, orientação operacional e melhores práticas, à medida que vão emergindo novas circunstâncias e requisitos.

1 https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection
2 https://au.int/sites/default/files/newsevents/reports/33025-rp-addis_ababa_declaration_of_the_stc-cict-2_en.pdf (Parág. 31)

Índice

Introdução 2
Índice 3
Resumo Executivo 4
Agradecimentos 6
Contexto Africano 7
Contexto da Política 7
Para uma consistência com os princípios da privacidade dos dados aplicados noutras regiões 9
Princípios identificados na Convenção de Malabo 9
Conjuntos de princípios similares de outras fontes 9
Quadros regionais e nacionais vigentes em África 10
Temas pelo Grupo de Partes Interessadas 11
Recomendações 19
Sobre a Internet Society 28
Sobre a Comissão da União Africana 28

Resumo Executivo

Esta secção resume as principais funções e responsabilidades dos principais grupos de partes interessadas, no que se refere à proteção dos dados pessoais.

Governos e responsáveis políticos

Função: habilitar o cidadão digital e assegurar que o ambiente em linha é de confiança, seguro e benéfico para todas as partes interessadas.

Responsabilidades:

- Aumentar o seu entendimento dos benefícios e perigos de uma economia orientada pelos dados;
- Compreender as forças económicas e sociais em acção no ecossistema dos dados pessoais;
- Cultivar um quadro social a longo prazo para a confiança na economia digital, assegurando que os benefícios são distribuídos com imparcialidade.

Estes são os objectivos dos princípios fundamentais e das medidas de habilitação e apoio.

Autoridades de Protecção de Dados (DPA)

Função: aumentar a certeza jurídica, aplicando as leis relativas à protecção de dados, investigar alegadas violações da privacidade, impor sanções quando aplicáveis e trabalhar com os grupos de partes interessadas e outras DPA.

Responsabilidades:

- Oferecer um contributo especializado aos governos relativamente à política e às leis da protecção de dados;
- Dar uma orientação clara aos responsáveis pelo tratamento de dados e aos fabricantes/programadores de produtos e serviços;
- Fazer uma aplicação eficaz dos regulamentos da protecção de dados, incluindo investigação e sanções;
- Desenvolver aconselhamento e ajuda para os titulares dos dados;
- Coordenar com outras DPA, a apoiarem as normas e a aplicação de protecção de dados transfronteiriças consistentes.

Responsáveis pelo tratamento de dados e os seus parceiros

Função: criar e aplicar práticas responsáveis e sustentáveis para o tratamento dos dados pessoais, que reflictam os interesses dos titulares de dados, bem como os dos responsáveis pelo tratamento de dados e os seus parceiros.

Responsabilidades:

- Maximizar a confiança, como uma expectativa do cidadão/cliente/utilizador, como um benefício oferecido pelos seus serviços e produtos e como um activo económico da sua organização. A confiança aumenta a reputação, reforça o consentimento e pode oferecer uma vantagem competitiva num contexto comercial;
- Procurar resolver os problemas práticos da protecção de dados pessoais (consentimento, prazos de conservação de dados, segurança dos dados, etc.), com a mistura certa de medidas técnicas e processuais;
- Aumentar o uso da Privacidade desde a Concepção (PbD) e de ilustração baseado no valor[3], como parte integrante do desenvolvimento do produto/serviço.

---

3 A maioria dos processos de concepção baseia-se principalmente em aspectos como a função, forma, estética e custo. A concepção baseada no valor reconhece que toda a escolha de concepção tem uma dimensão ética e integra sistematicamente considerações éticas no ciclo da concepção e do desenvolvimento.

Cidadãos e Sociedade Civil

Função: criar cidadãos digitais eficazes; tornar-se uma parte interessada activa da sua própria privacidade e dados pessoais.

Responsabilidades:

- Compreender os riscos envolvidos na vida em linha;
- Compreender e exercer os direitos relacionados com os dados pessoais, privacidade e autonomia;
- Desenvolver as suas capacidades para proteger os seus interesses em linha, seja directamente, ou usando ferramentas e serviços que ajudam a aumentar a sua privacidade;
- Desenvolver uma voz colectiva (com o consumidor e organizações da sociedade civil) para mudar o mercado do consumidor no sentido de uma melhor privacidade.

Tarefas das várias partes interessadas

Todas as partes interessadas têm colectivamente uma função de criar um ecossistema em linha de confiança que opere para benefício de todos.

A privacidade tem a ver com o respeito das expectativas dos indivíduos e como a sua informação pessoal é tratada; a privacidade depende de uma relação de respeito, entre o indivíduo e as partes interessadas que recolhem e usam os seus dados. Ocorre uma melhor privacidade em linha quando todos os que estão em causa são parte da solução.

Muitos problemas práticos da protecção de dados exigem uma acção de colaboração de mais do que uma parte interessada; por exemplo:

- Desenvolvimento de códigos de melhores práticas (DPA, responsáveis pelo tratamento de dados, organismos da indústria);
- Criação e administração de regimes de certificação para a protecção de dados (DPA, organizações de consumidores e organismos de padrões e certificação); e
- Consentimento do utilizador e respeito pelos contextos de privacidade[4] (DPA, responsáveis pelo tratamento de dados e organismos de consumidores).

Estas são as acções recomendadas sob o título “Soluções de várias partes interessadas”.

4 A privacidade é frequentemente uma questão de respeito pelo contexto em que a informação é divulgada e não a partilhar ou reutilizar noutros contextos (por exemplo, não pegar em dados clínicos privados e publicá-los num jornal).

Agradecimentos

Gostaríamos de agradecer os contributos inestimáveis de Robin Wilton (Internet Society), que trabalhou no primeiro projecto das directrizes e reviu os sucessivos projectos baseados no contributo de colaboradores especialistas. Gostaríamos também de agradecer os contributos dos seguintes, que participaram na workshop de especialistas para identificar e discutir os principais temas destas Directrizes e comentaram no projecto detexto:

Souhila Amazouz (CUA)
Yaovi Atohoun (ICANN)
Dawit Bekele (ISOC)
Alebachew Berhanu (Universidade Bahir Dar)
Betel Hailu (ISOC)
Verengai Mabika (ISOC)
Evelyn Namara (ISOC)
Marsema Tariku (ISOC)
Wakabi Wairagala (CIPESA)
Auguste Yankey (CUA)
Moctar Yedaly (CUA)
Kinfe Yilma (Universidade de Melbourne)

Outros contributos e/ou revisões dos sucessivos projectos, foram cuidadosamente feitos por:

Jacques Bus (Digital Enlightenment Forum)
Jemal Hussien (CUA)
Olaf Kolkman (ISOC)
Eve Maler (Forgerock Inc.)
Christine Runnegar (ISOC)
Colin Wallis (Kantara Initiative)
Pat Walshe (Privacy Matters Ltd.)
Sally Wentworth (ISOC)

Internet Society, Abril de 2018
Ref. do Documento: AUC-PDPG-Apr2018

Contexto Africano

Estas Directrizes têm em conta as seguintes características do contexto africano, conforme identificadas pelo grupo de especialistas:

- A significativa diversidade cultural e jurídica através do continente, com expectativas de privacidade diferentes;
- Variações no acesso à tecnologia e aos serviços em linha, entre os Estados-membros;
- Sensibilidades referentes à etnia e à definição do perfil sem consentimento, no contexto do estado nação;
- Níveis diferentes de capacidade em áreas como a tecnologia e a lei e administração relacionada com a tecnologia;
- Riscos decorrentes da elevada dependência de fabricantes e de fornecedores de serviços não africanos:
    - A capacidade limitada dos Estados-membros da União Africana de influenciarem o comportamento de fornecedores de serviços externos;
    - Risco potencialmente acrescido de uso indevido dos dados se o conteúdo e os serviços forem fornecidos unicamente por empresas estrangeiras (como serviços "over the top" ou OTT).

Estes factores podem aumentar a dificuldade da formulação e aplicação de uma política consistente entre e por vezes mesmo dentro, dos estados-membros.

Contexto da Política

Como a Convenção da União Africana sobre Cibersegurança e Protecção de Dados (2014) e a Declaração Ministerial de Adis Abeba (AU/CCICT-2, 2017) ilustram, as Directrizes foram desenvolvidas no contexto de uma alteração rápida no âmbito e na disponibilidade dos serviços en linha em África e o pano de fundo dos objectivos ambiciosos da política africana nos termos da Agenda 2063.

A UA devotou uma considerável atenção na política à harmonização. Por exemplo, o Acto Constitutivo da União Africana[5] (Artigo 3º, Página 6) refere explicitamente a coordenação e harmonização das políticas entre as Comunidades Económicas Regionais, existentes e futuras, em apoio de (entre outros) os seguintes objectivos:

- Uma África unida e forte
- Integração política e socio-económica acelerada do continente;
- Estabelecimento de condições que habilitem África a desempenhar o seu legítimo papel na economia global;
- Desenvolvimento sustentável ao nível económico, social e cultural.

A CUA está também a estabelecer a "Iniciativa de Carácter Político e Regulamentar para a África Digital" (PRIDA), no âmbito da qual serão exploradas as ferramentas e metodologias para a harmonização e coordenação da política e do regulamento.

Como parte de um objectivo de uma maior integração regional, a Assembleia da União, na sua 27ª Sessão Ordinária (Julho de 2016, Kigali, Ruanda), deliberou implementar um protocolo para a livre circulação de pessoas no continente.

5 https://au.int/sites/default/files/pages/32020-file-constitutiveact_en.pdf

- Esta resolução tem implicações no intercâmbio dos dados de identificação dos cidadãos respeitador da privacidade normalizada e segura, no contexto do cruzamento das fronteiras e do intercâmbio subsequente de dados pessoais através das fronteiras, quando um cidadão trabalha, reside ou faz transacções fora do seu país de origem. A mesma Sessão reconheceu a importância da livre circulação de bens e serviços como um elemento de integração e unidade continental mais profunda.
- O princípio da livre circulação de pessoas reflecte-se também no Art. 43º do Tratado que estabelece a Comunidade Económica Africana (1991, Abuja, Nigéria).

A UA também deu passos significativos no sentido do estabelecimento de uma Zona de Comércio Livre Continental (ZCLC) em apoio dos princípios de livre circulação de pessoas, bens e serviços, conforme refletido nas Decisões, Declarações e Resolução da sua 25ª Sessão Ordinária (Junho de 2015, Joanesburgo, África do Sul). Isto tem implicações na correspondente transferência transfronteiriça de dados pessoais, no contexto das transacções em linha (comércio) e dos indivíduos que vivem e trabalham nos Estados-membros que não sejam o seu país de origem.

Os Estados-membros da UA também têm obrigações relacionadas com as liberdades fundamentais e os direitos humanos, conforme estabelecido nas declarações e convenções da UA e das Nações Unidas. Isto inclui o compromisso de respeitar, proteger e promover o direito à privacidade e protecção dos dados pessoais. Num certo número de casos, o direito à privacidade já se encontra previsto nas constituições dos Estados-membros (por exemplo, Botswana, República Democrática do Congo, Egipto, Gana, Quénia, Nigéria, Sierra Leone, África do Sul, Tanzânia, Uganda, Zâmbia e Zimbabué reconhecem o direito à privacidade individual nas suas constituições nacionais como um direito humano fundamental).

Todas estas políticas e obrigações têm implicações em termos do intercâmbio seguro, transparente, robusto e respeitador da privacidade dos dados pessoais transfronteiriço e entre jurisdições. Isto, por seu turno, impõe um ónus nos Estados-membros de garantir que a evolução na direcção da integração regional, comércio livre e desenvolvimento não é impedido ou tornado mais arriscado, por uma incapacidade de trocar os dados pessoais de forma segura, fiável e com o devido respeito pelos direitos individuais.

Paralelamente, o uso seguro, robusto e respeitador dos dados pessoais é um potenciador essencial da capacidade dos Estados-membros da UA fazer o seguinte:

- Manter a sua própria autodeterminação na sociedade da informação e manter-se a par da rápida mudança;
- Capitalizar na inovação tecnológica;
- Criar e manter a confiança numa economia orientada pelos dados.

Para manter a confiança na economia orientada pelos dados, os membros da UA têm de reconhecer o papel que os dados pessoais desempenham e as forças económicas que geram. Quando bem sucedida, a economia orientada para os dados pode criar o crescimento económico, oferecer serviços irresistíveis e inovadores e melhorar a qualidade de vida.

Porém, a economia orientada pelos dados também pode ter um lado escuro, se os dados pessoais forem tratados de forma exploradora ou abusiva e se os interesses do titular dos dados forem lesados. O custo e o risco inerente nestes casos por vezes só se torna aparente quando as coisas correm mal, quando há uma violação de dados ou é exposta uma fraude. Isto pode ter um efeito profundo na confiança e segurança nos serviços em linha e o correspondente impacto numa economia orientada pelos dados. Estas Directrizes recomendam medidas para a redução do risco destes últimos resultados indesejados.

O grupo de especialistas não esqueceu que, para alguns Estados-membros e responsáveis políticos da UA, a protecção de dados pessoais pode ser um domínio relativamente desconhecido, o que pode ser uma barreira a uma iniciativa política eficaz. As Directrizes visam ajudar a habilitar os Estados-membros no desenvolvimento da política e das leis de protecção de dados pessoais. As recomendações são consequentemente, acompanhadas por um certo número de medidas de habilitação e de apoio, como programas focados no aumento da sensibilização e educação, para responsáveis políticos e indivíduos.

Finalmente, há o risco de impacto significativo (nos seus cidadãos e economias) se os Estados-membros da UA não fizerem nada. Em conformidade, as Directrizes propõem acções destinadas a mitigarem este risco.

Rumo a uma consistência com os princípios da privacidade aplicados noutras regiões

Princípios identificados na Convenção de Malabo

O Artigo 13º da Convenção identifica os seis princípios seguintes relativos à protecção dos dados:

- Consentimento e legitimidade;
- Tratamento legítimo e justo;
- Finalidade, relevância e conservação dos dados;
- Exactidão dos dados ao longo do seu ciclo de vida;
- Transparência do tratamento;
- Confidencialidade e segurança dos dados pessoais.

Conjuntos de princípios similares de outras fontes

Várias estruturas de privacidade nacionais e internacionais convergiram amplamente para formar um conjunto de princípios fundamentais de privacidade. Estes são implementados em quadros de privacidade nacionais em mais de 100 países. Os três mais proeminentes são talvez as Directrizes de Privacidade da Organização para a Cooperação e Desenvolvimento Económico (OCDE) (não vinculativas, alteradas pela última vez em 2013), a Convenção 108 do Conselho da Europa, que é vinculativa para os seus 51 signatários[6] e o Quadro de Privacidade da Cooperação Económica Ásia-Pacífico (APEC) e actualizada pela última vez em 2015. Estes documentos expressam princípios similares de privacidade e são amplamente reconhecidos como fornecendo a base fundamental para as políticas e práticas de privacidade em linha.

Com variações menores, constituem a base das directrizes aprovadas pela Assembleia Geral das Nações Unidas e pela Comunidade das Nações e estão amplamente alinhadas com o Regulamento Geral sobre a Protecção de Dados da União Europeia de 2016.

Eis as áreas centrais desses princípios de privacidade:

- **Limitação à recolha.** Os dados pessoais têm de ser obtidos e tratados de forma lícita, justa e, na medida do possível, transparente;
- **Qualidade dos dados.** Os dados pessoais têm de ser exactos no momento da recolha e terão de ser tomadas medidas razoáveis para assegurar que é mantida a sua exactidão durante o período da conservação;
- **Especificação da finalidade.** Os dados pessoais só podem ser recolhidos para as finalidades especificadas, explícitas e legítimas. Os dados pessoais só podem ser usados para outras finalidades que sejam compatíveis com as leis aplicáveis, como o arquivo de dados que seja do interesse ou para fins de investigação científica;
- **Limitação do Uso.** Os dados pessoais não podem ser divulgados, disponibilizados ou utilizados para outras finalidades salvo com o consentimento do indivíduo ou quando autorizado por lei;
- **Salvaguardas de Segurança.** Os dados pessoais devem ser protegidos por salvaguardadas razoáveis de segurança para manter a sua integridade e confidencialidade.
- **Abertura.** Deve haver uma política geral de abertura sobre desenvolvimentos, práticas e políticas relativamente aos dados pessoais.

6 À data da publicação destas Directrizes

- **Participação individual.** Os indivíduos têm de ter o direito de obter informação sobre os seus dados pessoais detidos por outros. Estes dados têm de ser fornecidos dentro de um prazo razoável, de uma forma que seja facilmente legível e a um custo que não seja excessivo. Os titulares dos dados têm o direito de contestar os seus dados e que os mesmos sejam alterados se forem incorrectos ou apagados se isso for apropriado;
- **Responsabilidade**. Aqueles que recolhem e tratam os dados pessoais têm de ser capazes de demonstrar a sua conformidade com estes princípios.

O alinhamento com estes seis princípios estabelecido no Artigo 13º da Convenção não é exacto, mas há uma enorme semelhança. Duas áreas de diferenciação são as seguintes:

- O Artigo 13º da Convenção de Malabo lista o "Consentimento" como um princípio separado, enquanto nos quadros da OCDE e do Conselho da Europa, o consentimento é incluído como um critério do tratamento lícito;
- Os Artigos 7º e 10º da Convenção 108 do Conselho da Europa, o Princípio 14 das Directrizes de Privacidade da OCDE e o parágrafo 32 do Quadro de Privacidade da APEC, expressam os requisitos referentes à responsabilidade do responsável pelo tratamento. A responsabilidade não está explícita nos príncipios da Convenção de Malabo (Artigo 13º) ou nas Obrigações do Responsável pelo Tratamento de Dados Pessoais (Artigos 20º-23º) Porém, os Artigos 16º-19º implicam a responsabilidade por parte do responsável pelo tratamento, expressando certos direitos por parte titular dos dados (exactidão dos dados, correcção, apagamento, etc).

Estas variações são relativamente menores e não devem suplantar o facto que haja muito mais semelhança e alinhamento que divergência. Não obstante, sugerimos que os os Estados-membros da UA prestem particular atenção aos mecanismos de responsabilidade para os responsáveis pelo tratamento nos seus respectivos quadros de protecção de dados, para que este importante tópico não deixe de ser abordado.

Quadros regionais e nacionais vigentes em África

A pesquisa realizada pela CIPESA relativamente a estas directrizes identificou os quadros africanos seguintes que refectem os princípios de privacidade e protecção dos dados similares aos indicados supramencionados:

- Lei Modelo da SADC sobre a Protecção dos Dados (2010);
- Lei Suplementar da CEDEAO A/SA.1/01/10 sobre a Protecção de Dados Pessoais (2010);
- Quadro da CAO para Ciberleis (2008)

De acordo com a mesma pesquisa, os países seguintes têm legislação vigente ou proposta (no momento em que estas Directrizes são escritas) que integra princípios similares relativamente aos direitos dos titulares dos dados sujeitos e ao estabelecimento de autoridades de protecção de dados: Angola (2016), Guiné Equatorial (2016), Mauritânia (2017), África do Sul (2013), Burkina Faso (2004), Mali (2013), Gabão (2011), Benim (2009), Gana (2012), Cote d´Ivoire (2013), Lesoto (2012), Madagáscar (2014), Marrocos (2009), Senegal (2008), Tunísia (2004), Zimbabué (2003). As propostas de lei da privacidade e protecção dos dados no Quénia, Níger, Nigéria, Tanzânia e Uganda também têm disposições similares.

Temas pelo Grupo de Partes Interessadas

Esta secção das Directrizes reflete os tópicos e questões levantadas durante o processo de consulta e no ateliê dos peritos.

Estão agrupados por tipo de partes interessadas e, dentro de cada secção de partes interessadas, os temas estão ordenados de acordo com os artigos correspondentes da Convenção. O objectivo desta secção é fornecer contexto e informação sobre os antecedentes para as Recomendações apresentadas na secção subsequente.

Governos e Responsáveis políticos

Tema	Observações
Quadros e fluxos dos dados transfronteriços	O Regulamento que é proporcional ao de outras jurisdições contribui para a confiança mútua e estabelece a base para um intercâmbio de dados com confiança, incluindo (mas não estando limitado) aos dados pessoais. A protecção de dados pessoais é, consequentemente, um potenciador de uma maior confiança na circulação transfronteiriça de pessoas, bens e serviços.
Harmonização (Convenção de Malabo, Preâmbulo, Parág. 20)	O Preâmbulo da Convenção refere-se à desejabilidade de uma ciberlegislação harmonizada. Sobre o mesmo princípio, medidas para o aumento da consistência na legislação da protecção de dados entre os Estados-membros ajudará a reduzir ou mitigar as assimetrias na protecção da privacidade. As estratégias, políticas e leis de Protecção dos Dados Pessoais devem procurar abranger as seguintes áreas: • Aumento da consciência das obrigações e direitos da protecção de dados pessoais; • Objectivos e quadros da política; • Leis e autoridades de protecção dos dados; aplicação e sanções. Os Estados-membros da UA necessitarão de colaborar para alcançar esta consistência. Espera-se que a iniciativa PRIDA da CUA seja um importante potenciador desses esforços.
Direitos e prerrogativas dos cidadãos do Estado (Convenção de Malabo, Preâmbulo e Art. 8º)	A Convenção reafirma o empenho dos Estados-membros da UA de respeitar as liberdades fundamentais e os direitos humanos e a Carta Africana sobre os Direitos Humanos e dos Povos. Um princípio importante é assegurar que os indivíduos gozem de direitos equivalentes online e offline. Além disso, a Convenção também se refere às prerrogativas do Estado, pelas quais se entende que o direito à privacidade é um direito qualificado, legitimamente afastado, nalgumas circunstâncias, no interesse da segurança nacional, aplicação da lei e segurança pública. Isto coloca um desafio de administração em termos de: • Estabelecer condições consistentes e exequíveis sob as quais essas excepções à lei da protecção de dados podem ser permitidas; • Criar um regime de supervisão robusto e fiável para monitorizar o uso dessas excepções, particularmente no contexto da segurança nacional, onde o acesso à informação de administração relevante pode ser constrangida (por razões compreensíveis).

A assimetria e reciprocidade entre os níveis de protecção proporcionados pelos Estados-membros da UA, e entre os Estados- membros da União Africana e outras entidades (Convenção de Malabo, Art. 10º.6.k)	É provável que existam assimetrias no nível da protecção de dados proporcionado pelos membros da UA, mas os seus efeitos podem ser mitigados e/ou reduzidos, através de uma atenção adequada à administração, medidas reguladores e de aplicação e factores económicos. O Article 10º.6.k da Convenção menciona acordos de privacidade para a transferência de dados fora da UA. A reciprocidade é um factor essencial na redução da assimetria na protecção de dados pessoais. Critérios de adequação consistentes (entre os Estados-membros) para o tratamento de dados pessoais são um mecanismo importante para assegurar a reciprocidade prática nas medidas legais e de aplicação. (Porém, esta é apenas uma abordagem. Na região Ásia-Pacífico, por exemplo, em vez de visar decisões de adequação como base para as transferências transfronteiriças, a APEC desenvolveu um mecanismo voluntário baseado na responsabilidade, conhecido como o Sistema de Normas de Privacidade Transfronteiriça da APEC (sistema CBPR) e o Reconhecimento de Privacidade da APEC para Subcontratantes (Sistema PRP).

Responsáveis pelo Tratamento de Dados

Tema	Observações
Funções e obrigações	O comportamento dos responsáveis pelo tratamento de dados é motivado por diversos factores (como rentabilidade, eficiência, benefício social e da comunidade) dependendo frequentemente em primeiro lugar em comoo responsável pelo tratamento de dados opera num sector comercial, público ou não público, por exemplo. O seu comportamento será também constrangido, em princípio pela lei aplicável, mas apenas se a lei for efectivamente aplicada. Neste contexto, a lei habitualmente só pode estabelecer um limiar mínimo para que o comportamento do responsável pelo tratamento de dados seja aceitável. É provável que uma protecção da privacidade verdadeiramente eficaz exija que os responsáveis pelo tratamento de dados excedam o limiar puramente legal e adoptem boas práticas para o tratamento de dados, como a participação no esquema de certificação para a protecção dos dados pessoais. Isto pode ser considerado, os termos da Convenção, como uma protecção de dados equivalente ao pedido (no Artigo 2º) para o desenvolvimento de códigos de conduta harmonizados no domínio da cibersegurança.
Relação entre os responsáveis pelo tratamento e os subcontratantes	Em relação aos dados pessoais: • Responsável pelo tratamento de dados significa uma pessoa que determina as finalidades para as quais e a forma pela qual quaisquer dados pessoais são, ou devam ser, tratados. • Subcontratante significa qualquer pessoa (à excepção de um funcionário do responsável pelo tratamento de dados) que trate os dados em nome do responsável pelos dados. Como princípio geral, o responsável pelo tratamento de dados não deixa de ter quaisquer obrigações quando passa os dados pessoais a um subcontratante para proceder ao tratamento em seu nome. O subcontratante também "herda" as responsabilidades do responsável pelo tratamento de dados no que se refere à protecção dos dados que lhe foram passados e à privacidade do titular dos dados. Porém, por exemplo, o subcontratante não será responsável por dar resposta aos pedidos de acesso dos titulares dos dados (SAR) referentes a dados pessoais que lhe foram passados: o subcontratante pode legitimamente remeter esse pedido para o responsável pelo tratamento. (Os SAR serão mencionados com mais detalhe abaixo, da perspectiva do responsável pelo tratamento e da autoridade de protecção de dados).

Consentimento (Artigo 13º, Princípio 1)	A obtenção do consentimento para o tratamento dos dados pessoais apresenta desafios éticos, jurídicos e práticos. Uma legislação bem intencionada pode dar aos responsáveis pelo tratamento um incentivo perverso para soluções que minam a confiança em vez de a reforçar. Por exemplo, a União Europeia introduziu uma "lei relativa a cookies" que se destinava a impedir os websites de rastrearem os utilizadores sem o seu conhecimento ou consentimento, usando pequenos pedaços de dados identificáveis (cookies) armazenados no navegador do utilizador. Alguns websites responderam apresentando uma opção de consentimento "pegar ou largar" que não dava aos utilizadores uma opção séria. Isto pode ter obedecido à letra da lei, mas não implementa o seu espírito. Em geral, os utilizadores não obtiveram, consequentemente, melhores resultados em termos de privacidade. A resolução do problema difícil do consentimento é provável que exija uma combinação de medidas legais e técnicas e, nalguns casos, uma contrapartida aos fortes incentivos económicos que os prestadores de serviços possam ter para "contornar" a lei. As leis da protecção de dados devem ser desenvolvidas através de um processo que estabeleça o equilíbrio entre o que é legalmente exigido e o que é tecnicamente possível e o que melhor representa os interesses do indivíduo a quem é pedido que dê o consentimento. Em alguns regulamentos da protecção de dados, como a Convenção 108 do Conselho da Europa, o requisito para o consentimento ainda é mais limitado (exigindo, por exemplo, que o consentimento seja informado, específico , revogável, etc.) cada uma destas condições terá implicações que podem exigir medidas legais, técnicas e processuais a implementar pelo responsável pelo tratamento. Este problema, amplamente, ainda carece de soluções definitivas e os Estados-membros são encorajados a incentivarem uma investigação multi-disciplinar quanto às melhores formas de o abordar.
Fluxos dos dados pessoais entre contextos e o seu impacto na privacidade (Art. 13º, Princípio 2 - Lealdade do tratamento)	A integridade contextual é importante.[7] Os dados pessoais que são recolhidos num contexto e depois usados noutro contexto sem a consciência e consentimento das violações individuais da privacidade do indivíduo (por exemplo, os dados pessoais que são partilhados por um utilizador para preencher uma transacção comercial em linha, mas são vendidos a um anunciante sem o conhecimento do indivíduo). Esta noção de integridade contextual implica um dever do responsável pelo tratamento de estar ciente do contexto em que os dados são recolhidos e a respeitar a integridade daquele contexto. Isto está relacionado com o princípio da privacidade da "finalidade da recolha". Como frequentemente há fortes incentivos para os responsáveis pelo tratamento transferirem os dados de um contexto para outro (por exemplo, retirar os dados das transações dos clientes e vendê-los para que possam ser usados para publicidade direccionada), as políticas da protecção de dados têm de assegurar que isto nunca é feito em detrimento do titular de dados, ou assegurar que o titular de dados tem oportunidade de expressar e aplicar as preferências sobre se, quando ou como isto deve acontecer. A transferência de dados entre os diversos contextos é um problema, especialmente, quando os utilizadores não têm conhecimento que isto está a acontecer. Por exemplo, uma criança a quem é dado um urso de peluche "ligado" pode não compreender que o urso liga o contexto "de casa" privado a um contexto comercial terceiro. Os utilizadores do monitor de actividade física Strava parecem não se ter apercebido que o dispositivo estava a tornar possível retirar os dados de localização de um contexto (como uma base militar activa) e torná-los públicos noutro (mapas pesquisáveis em linha). Uma vez que os utilizadores frequentemente têm pouco controlo sobre o uso subsequente de dados que divulgam, muita da responsabilidade pelo uso apropriado de dados recai sobre o responsável pelo tratamento de dados. Os governos devem encorajar uma cultura de ética ou baseada desde a concepção nos valores[8], assegurando que os prestadores de serviço estão cientes das escolhas desde a concepção que integram a privacidade e outros princípios éticos nos produtos e serviços que tratam os dados pessoais.
Os pedidos de acesso dos titulares dos dados (Convenção de Malabo, Artigos 16º-19º) e a sua relação com a responsabilidade e a transparência	A maioria das leis da protecção de dados integram um princípio de responsabilidade, conforme definido, por exemplo, nas Directrizes de Privacidade da OCDE. As Directrizes da OCDE também indicam a transparência como um elemento essencial da responsabilidade. Para os responsáveis pelo tratamento isto implica (entres outros) uma obrigação de responder aos pedidos dos titulares dedados sobre os dados que são detidos sobre os mesmos. Isto, por seu turno, implica uma obrigação dos responsáveis políticos assegurarem que os pedidos de acesso dos titulares de dados são abordados num quadro legal que assegure que são tratados de uma forma que sirva os interesses legítimos dos titulares dos dados e que não imponha obstáculos ao titular dos dados ou ónus indevido ao responsável pelo tratamento.

7 "Privacidade como Integridade Contextual" (Helen Nissenbaum, Washington Law Review, 2004)
8 Ver, por exemplo, "Inovação Ética nas TI" (Sarah Spiekermann, 2016)

Confidencialidade do tratamento de dados e medidas apropriadas para proteger os dados (Artigos 20º-21º e Artigo 15º referente à possibilidade de ligação)	A Convenção obriga os responsáveis pelos dados a tomar medidas apropriadas para proteger os dados pessoais, assegurando a sua confidencialidade e integridade. "Medidas apropriadas" incluirá um conjunto de opções técnicas, processuais e físicas. Por exemplo, registos em papel fechados num armário de arquivo estão protegidos por uma forma de controlo de acesso; os registos digitais por detrás de fortes medidas de autenticação e autorização[9] têm outra forma de protecção; ficheiros que estão encriptados, depois outra e assim por diante. Os responsáveis pelo tratamento devem ser encorajados a aplicar as normas das melhores práticas à protecção de dados. A este respeito muitos países adoptaram a abordagem baseada no risco, em que as medidas consideradas apropriadas são avaliadas em termos de risco, probabilidade e potencial impacto da não protecção dos dados pessoais em questão. Os três factores "clássicos" da segurança são todos relevantes neste contexto: confidencialidade, integridade e disponibilidade. Os dados têm de ser protegidos contra a divulgação indesejada, alteração indesejada e destruição/inacessibilidade indesejada. Os Estados-membros devem remeter para a correspondente orientação de cibersegurança nestes tópicos. Também sob o título da cibersegurança, os responsáveis pelo tratamento de dados e, se necessário, as autoridades de protecção de dados devem procurar orientação referente à fiabilidade dos mecanismos de segurança (algoritmos, comprimento das chaves e disciplinas de gestão da chave) a nível nacional e internacional. Exemplos de fontes dessa orientação, noutras regiões, são: • ENISA (Agência da União Europeia para a Segurança das Redes e da Informação) • NIST (Estados Unidos, mas para a qual remetem muitos outros países) • CESG (orientação específica para o Reino Unido, por exemplo, para a indústria do Reino Unido) Essa orientação ajudará as autoridades nacionais a medir, por exemplo, o período durante o qual uma determinada forma de encriptação deve ser considerada um mecanismo de protecção fiável para os efeitos dos Artigos 20º-21º. De igual modo, se forem usadas técnicas de pseudonimização e/ou anonimização como meio de protecção dos dados pessoais contra divulgação ou uso indesejado, a sua eficácia deve ser monitorizada à luz dos avanços nas técnicas para "re-identificação" de dados supostamente anonimizados ou pseudonimizados. Para além da re-identificação, devem ser consideradas neste contexto outras duas ameaças à privacidade: inferências e possibilidade de ligação. • A inferência refere-se à possibilidade de tomar dados não pessoais e usá-los para derivar assunções e predições pessoais, ou tomar os dados pessoais e usá-los para derivar dados pessoais sensíveis sobre alguém. Por outras palavras, os dados que possam não parecer pessoais podem de facto ser, ou podem ser usados para inferir dados que sejam pessoais. De igual modo, dados pessoais "normais" podem ser o ponto de partida para inferir dados pessoais sensíveis. Os Estados-membros devem rever a legislação da protecção de dados para verificar se indivíduos ou grupos estão protegidos de serem seleccionados ou discriminados, através do uso desses dados derivados ou inferidos. • A possibilidade de ligação refere-se à possibilidade dos responsáveis pelo tratamento ou terceiros estabelecer que dados pessoais de diferentes fontes estão relacionados com o mesmo indivíduo. Por exemplo, que os registos de chamadas para este número de telefone estão relacionados com o mesmo indivíduo que as publicações naquele site das redes sociais. Uma ligação de dados, desta forma, pode subverter gravemente a privacidade e a autonomia do indivíduo, impedindo-as de manter contextos discretos na sua vida em linha. Estas são áreas de dificuldade em que para legislar com sucesso, particularmente quando a tecnologia referente à inferência (inteligência artificial, processo de decisão algorítmico, aprendizagem pela máquina) está a evoluir tão rapidamente e quando é tão fácil minar dados para os tipos de ligação descrita acima. Em conformidade, recomendamos uma abordagem ao problema por múltiplas partes e a busca de soluções baseadas na capacidade de combinar medidas regulamentares, processuais, técnicas e educativas, conforme necessário. A abordagem baseada no risco é provavelmente a que oferece melhores resultados.

9 Autenticação é o processo de validação que alguém é quem alega ser, no momento em que tenta aceder a um serviço ou recurso. Autorização é um processo de estabelecimento que um utilizador autenticado tem o direito de aceder ao serviço ou recurso em questão. Controlo de acesso é o processo de aplicação daquele direito.

Períodos de conservação (Convenção de Malabo, Art. 22º)	A maioria das leis da protecção de dados actuais incorporam o princípio do estabelecimento de limites à conservação de dados. Porém, poucos responsáveis pelo tratamento de dados põem em prática o princípio e, consequentemente, muitos dados são mantidos por um período superior ao necessário (por vezes indefinidamente) colocando os responsáveis pelo tratamento em risco acrescido de violação dos dados pessoais e os titulares de dados em risco de violação da privacidade. O regime regulador e de supervisão não deve basear-se na assunção que os dados serão apagados por defeito, devendo assim incluir medidas que encoragem a minimização de dados e o apagamento e assegurar o cumprimento daquele princípio.
Sustentabilidade do acesso aos dados (Convenção de Malabo, Art. 23º)	O responsável pelo tratamento está obrigado, nos termos da Convenção, a assegurar que os dados pessoais permaneçam tecnicamente acessíveis. Em termos de privacidade, isto terá importância na capacidade do responsável pelo tratamento de cumprir os diversos requisitos dos Artigos 16º-19º da Convenção (direitos de notificação, acesso, correcção, apagamento, etc.). Também pode ser um factor no cumprimento dos Pedidos de Acesso do Titular de dados (Artigo 17º): o Artigo 17º não servirá os interesses do titular de dados se os responsáveis pelo tratamento de dados puderem responder aos pedidos de acesso do titular de dados de uma forma ou num formato que o titular de dados não possa usar.

Autoridades de Protecção de Dados

Tema	Observações
Elementos do regime de governação (Artigos 10º-12º)	Se as partes interessadas tiverem uma função legal ao abrigo das leis da privacidade e da protecção dos dados pessoais, a conformidade com os requisitos legais tem de estar sujeita a monitorização e aplicação; isto está directamente relacionado com o princípio da Responsabilidade da protecção de dados. Se as partes interessadas tiverem obrigações contratuais ou baseadas nas normas, terá de ser possível auditar a sua conformidade, o que implica a presença de assessores e auditores qualificados e capazes. Estas entidades devem consequentemente ser adicionadas à lista de partes interessadas, como se segue: • Titulares dos Dados, • Responsáveis pelo Tratamento de diversos tipos (fornecedor de identidade, fornecedor de atributo, fornecedor de serviço), • Autoridades de Protecção de Dados, • Assessores de Conformidade, • Auditores de Cumprimento e • Entidades de Acreditação para Assessores e Auditores. Isto também implica que as autoridades de protecção de dados tenham poder para investigar os processos de acreditação, avaliação e auditoria e penalizar os incumprimentos. Esse regime pode formar a base para o regime de certificação, para padronizar e implementar os princípios da protecção de dados. Um regime de certificação poderia cobrir também as funções conexas, como as disciplinas da segurança da informação, que são vitais para estabelecer o que constituem "medidas apropriadas" nos termos dos Artigos 20º-21º (e relevantes para os Artigos 15º e 23º). No contexto de cada Estado-membro, o regime de certificação para estas disciplinas permitiria que fossem desenvolvidos regulamentos e orientação para: • Confidencialidade, integridade e disponibilidade de serviços para o tratamento de dados. • Avaliação e selecção de algoritmos criptográficos, comprimentos de chave e procedimentos de gestão de chave. • Medição da força relativa dos diferentes mecanismos de autenticação. • Protecção dos dados pessoais através da anonimização e da pseudonimização. • Critérios de avaliação de risco para re-identificação dos dados anonimizados/pseudonimizados. • Critérios de avaliação de risco referentes aos dados de inferência e possibilidade de ligação. A certificação pode então formar a base para a concessão de uma marca de confiança aos interessados que cumpram os critérios especificados, que, por sua vez, pode ajudar a informar e orientar os indivíduos sobre as decisões de confiança que fazem em linha.

Função e independência das DPA (Artigo 11º)	A autoridade de proteção de dados (DPA) pode não cumprir o fim a que se destina se puder ser objecto de pressão política, administrativa ou comercial indevida. Por exemplo, se o pessoal estiver sujeito a nomeação/demissão arbitrária, se for privado dos seus poderes coercitivos ou recursos, ou se estiver sujeito a lobbying comercial ou a litígios vexatórios.
Decisões de Adequação (Artigo 12º.2.k)	DPA eficazes são o elemento chave para assegurar que as transferências de dados transfronteiriças acontecem num quadro de confiança mútua e normas consistentes (ver também as Observações acima, sob Governos e os Responsáveis Políticos, relativos à reciprocidade).
Direitos dos titulares dos dados (Artigos 13, 16-19)	As DPA terão uma função essencial a desempenhar no esclarecimento, comunicação, monitorização e aplicação dos direitos dos titulares de dados, conforme descrito em múltiplos artigos/disposições da Convenção. Article 18º: o direito de se opor ao tratamento. As DPA terão alguma responsabilidade na aceitação com fundamentos legítimos dessas objecções e uma responsabilidade considerável na determinação de quando é prático e razoável exercer esse direito (por exemplo, em que momento pode ser assumido que um titular de dados aceitou implicitamente no tratamento e sob que circunstâncias deve ser feito um pedido explícito de consentimento?). Artigo 19º: o direito de rectificação/apagamento. Poderá ser solicitado às DPA que dêem orientação, por exemplo, em circunstâncias sob as quais os dados pessoais possam/tenham de ser apagados a pedido do titular de dados, mesmo que os dados em questão sejam verdadeiros e exactos. Por exemplo, em que momento pode um titular de dados pedir que os dados pessoais sejam apagados com fundamento que o responsável pelo tratamento já não necessita dos mesmos e se o titular de dados e o responsável pelo tratamento de dados discordarem sobre esta matéria, quem deve resolver a discórdia? O direito ao apagamento deve ser distinguido do direito à desindexação (por vezes enganadoramente referida como o "direito de serem esquecidos"[10]). Desindexação do conteúdo web, no contexto da privacidade, é uma forma de tornar determinados dados menos acessíveis em linha. Nos termos da lei da UE[11], foi usado para exigir que os motores de busca suprimam os resultados de certas pesquisas indexadas no nome do titular dos dados. Isto não impede que a informação seja publicada na Web, nem garante que a informação não possa ser encontrada. Entre outras, a Lei Suplementar da CEDEAO sobre a Protecção de Dados[12] inclui disposições amplas, que podem ser usadas para introduzir um direito similar.

10 "Hiding In Plain Sight" (Garstka, Erdos, University of Cambridge 2017) dá uma explicação minuciosa da de-indexação vs. "direito a serem esquecidos": https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3043870
11 A Sentença "Google contra Espanha", 2014 http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065
12 Lei Suplementar A/SA.1/01/10 sobre a Protecção de Dados Pessoais no âmbito do ECOWAS (2010)

Cidadãos e Sociedade Civil (artigos 8º.1, 8º.2)

Tema	Observações
Direitos e correspondentes responsabilidades de aprender e ser informado	O volume da responsabilidade prática de proteger a privacidade pode ser visto a recair nos responsáveis pelo tratamento de dados e nas autoridades da protecção de dados. Isto reflecte a assimetria inerente na relação entre os titulares de dados e as empresas e entidades do sector público que tratam os seus dados. Os titulares de dados têm uma capacidade prática ou técnica muito pequena para proteger os seus dados pessoais depois de serem recolhidos. Porém, os indivíduos também são partes interessadas e, não apenas no sentido de conseguirem que as coisas sejam feitas ou dos seus dados pessoais. Os indivíduos não podem exercer direitos dos quais não têm conhecimento e os consumidores não podem influenciar o mercado através do seu comportamento se não estiverem suficientemente informados sobre as escolhas que fazem enquanto consumidores. Os indivíduos precisam de estar habilitados para serem cidadãos/consumidores digitais informados e estar cientes, por exemplo, do negócio em que entram quando subscrevem serviços "gratuitos" ou participam em plataformas de redes sociais que monetizam os seus dados. Além disso, os cidadãos também têm uma expectativa legítima que podem, fazer as suas coisas em linha em segurança, pelo que os legisladores e as autoridades de supervisão têm o correspondente dever de garantir que os cidadãos não são colocados em risco de dano indevido pelo uso das TIC e da economia digital. As assimetrias de poder e informação podem representar uma barreira significativa a este respeito, uma vez que podem: • Impedir o comportamento do consumidor de exercer a influência devida no mercado; • Mascarar os efeitos de modelos comerciais de exploração ou predatórios; • Minar a confiança no comércio electrónico e noutros serviços em linha; • Impedir África de colher os benefícios da transformação digital. Os mesmos tipos de assimetria podem também corroer a confiança nas relações entre o cidadão e os serviços públicos. Quando este desgaste da confiança se torna sistémico, seja nos sectores comerciais ou públicos, os benefícios esperados da economia digital não podem ser concretizados Os tipos de regime de certificação e de marca de confiança descritos acima, sob "Elementos do regime de governação", são uma parte importante da criação e manutenção da relação de confiança entre os indivíduos e os serviços em linha.
Conselho independente e criação de capacidade	Os indivíduos necessitam de ajuda e encorajamento nos seus esforços de estarem mais bem informados sobre a proteção de dados pessoais e a sua relevância para a privacidade. A sociedade civil tem um papel a desempenhar ajudando a assegurar que se encontra disponível pesquisa, análise, relatórios e defesa independentes e que os indivíduos estão motivados para aprender e proteger a sua privacidade em linha.
Representação dos interesses dos interessados	As Organizações da Sociedade Civil (OSC) e a comunidade académica têm um importante papel a desempenhar no contexto africano, ajudando a assegurar que os esforços de privacidade e protecção de dados não são prejudicadas pela dimensão e diversidade do continente. A este respeito, incentivamos as organizações da sociedade civil a reunir a nível nacional e regional, tirando partido dos agrupamentos regionais existentes no âmbito da UA. Outros agrupamentos podem ser também valiosos, de modo a representarem mais eficazmente os interesses de grupos específicos de partes interessadas, como as mulheres e crianças, pessoas portadoras de deficiência, aqueles que se encontrem em risco de ciberbullying, etc.

Defesa Independente	Os OSC podem prestar um serviço valioso na realização de avaliações independentes do estado actual das leis da protecção de dados e da privacidade, incluindo uma análise comparativa com outros Estados-membros e outras regiões/continentes. Tem também uma função potencial no fornecimento de contributos para processos estabelecidos como a Avaliação Universal pelos Pares da ONU. Para a sociedade civil ser eficaz nesta função, os governos têm também de fazer a sua parte para assegurar que os OSC têm um ambiente seguro e construtivo onde trabalhar, com protecção apropriada contra assédio e interferência.

Recomendações

Bases: Privacidade, Confiança e Uso Responsável

Privacidade como base para a confiança no ambiente digital

Recomendação: Incentivamos os Estados-membros da UA, que nas suas medidas para ratificar e implementar as disposições da Convenção de Malabo, sejam explícitos que a protecção da privacidade em linha e dos dados pessoais é não só um direito fundamental, mas também um processo vital a longo prazo destinado a cultivar e a manter a confiança no uso das TIC, como pré-requisito para o desenvolvimento continuado da Sociedade da Informação em África. Isto é particularmente importante no que se refere a factores sociais como a etnia, vulnerabilidade, incapacidade e desvantagem.

Uso sustentável e responsável dos dados pessoais numa economia orientada pelos dados.

Recomendação: Os governos e as autoridades de protecção dos dados devem monitorizar a economia orientada pelos dados relativamente às práticas potencialmente lesivas no que se refere aos dados pessoais, como as seguintes:

- Práticas de recolha de dados e de monetização que destorçam o mercado e resultem na falta de escolha do consumidor;
- As práticas de utilização de dados que suscitam riscos não geridos (por exemplo, uma pequena empresa empreendedora que acumule muito mais dados do que os recursos ou competências que tem para os gerir; ou uma grande empresa que consolida quantidades massivas de dados num único alvo irresistível).
- Os modelos comerciais predadores ou exploradores que carecem de transparência e responsabilidade sobre a recolha e uso dos dados pessoais.

Quando possível, os governos e as autoridades de protecção de dados devem agir para corrigir práticas como as descritas, tendo devida atenção aos benefícios da inovação, da concorrência e de modelos comerciais sustentáveis. É provável que aplicação efectiva de medidas preventivas exija um conjunto de princípios e normas mutuamente acordados que rejam as transferências transfronteiriças dos dados pessoais.

Partes Interessadas: Governos e Responsáveis políticos

Maior consistência na protecção dos dados pessoais em toda a África

Recomendação:

- Desenvolver uma abordagem consistente: à política e à protecção dos dados pessoais; estabelecimento de autoridades reguladores e aplicação de medidas (isto é, descrito com mais detalhe abaixo, sob AUTORIDADES DE PROTECÇÃO DE DADOS).
- Desenvolver critérios comuns e consistentes para avaliar a adequação do nível da protecção dos dados pessoais para permitir as transferências transfronteiriças na UA.

Estes são factores importantes para assegurar que há reciprocidade entre os Estados-membros no que se refere:

- Os termos e condições ao abrigo dos quais os responsáveis pelo tratamento operam;
- Os direitos e condições gozados pelos indivíduos no que se refere à recolha e uso dos dados pessoais;
- As medidas de execução e as medidas jurídicas corretivas disponibilizadas aos titulares de dados.

Os estados-membros devem tomar devida nota da iniciativa PRIDA da AUC à medida que se desenvolve, assegurando que se colocam de forma a tirar partido das oportunidades que apresenta para um trabalho de colaboração

Os Estados-membros devem tomar devida nota da iniciativa PRIDA da CUA à medida que se desenvolve, assegurando que se colocam de forma a tirar partido das oportunidades que apresenta para um trabalho de colaboração harmonizar a política e o regulamento nesta área. [CM - Preâmbulo pg. 3 e Artigo 10º.6]

Respeito pela privacidade online e offline

Recomendação: Os estados-membros têm de respeitar e proteger os direitos dos indivíduos à privacidade online e offline. Devem rever as suas leis, procedimentos e práticas, incluindo os relacionados com a vigilância ou intercepção de comunicações, para assegurar o cumprimento eficaz dessas obrigações.

Excepções às leis da privacidade e protecção dos dados

Recomendação: Os Estados-membros só devem permitir excepções à aplicação das leis da privacidade e da protecção dos dados pessoais por razões de soberania nacional, segurança nacional ou segurança pública, em que satisfaça um objectivo legítimo, seja necessário, proporcional e não arbitrário. Os membros devem garantir que quaisquer poderes que estejam isentos da aplicação das leis da privacidade e da protecção dos dados estão sujeitos a um regime de supervisão judicial fiável e independente que ofereça transparência e responsabilidade. [CM - Preâmbulo pg. 2, pg. 3].

Partes Interessadas: Responsáveis pelo Tratamento e Subcontratantes

Pedidos de Acesso do Titular de Dados (SAR) - perspectiva do Responsável pelo Tratamento

Recomendação: Os responsáveis pelo tratamento têm de ser obrigados a responder aos SAR de uma forma ou num formato que o titular de dados possa tratar. De outra forma há o risco de o Artigo 17º não servir os interesses do titular de dados.

Contribuir para soluções de múltiplas partes

Recomendação: Se os problemas da protecção de dados exigirem soluções coordenadas ou de múltiplas partes, os responsáveis pelo tratamento devem desempenhar o seu papel nos processos de definição do problema, consenso sobre as opções disponíveis e implementação de soluções. Isto aplica-se particularmente às áreas descritas em mais detalhe na secção abaixo, em soluções de múltiplas partes interessadas:

- Melhores práticas, códigos de conduta e certificação;
- Consentimento;
- Respeito pela integridade contextual;
- Respostas aos SAR;
- Confidencialidade e integridade dos dados pessoais; e
- Períodos de conservação.

Os Responsáveis pelo Tratamento de dados devem prestar particular atenção aos avanços nas melhores práticas, como a privacidade desde a concepção e a privacidade predefinida. Estes são, entre outros, factores importantes para determinar quando não recolher ou conservar os dados.

As decisões de recolha , tratamento ou conservação dos dados habitualmente decorrem de uma série de outras escolhas de concepção e implementação, que tenham sido feitas ao longo do processo de desenvolvimento do produto. Os Responsáveis pelo Tratamento de dados devem tirar partido do volume crescente de orientações sobre a concepção do sistema baseado nos valores ou na ética para incorporar princípios de melhoria da privacidade nos seus produtos desde as fases iniciais. Isto reduzirá o custo subsequente de alcançar a conformidade com os requisitos da protecção de dados e suscita um crédito de confiança dos utilizadores.

Partes Interessadas: Autoridades de Protecção de Dados

Função e independência das autoridades de protecção de dados

Uma autoridade de protecção de dados (DPA) nacional independente é um elemento vital do quadro legal e institucional para a criação de confiança online, conforme previsto da Convenção de Malabo (Artigos 10º-12º).

Recomendações: O cargo de comissário da DPA deve ser preenchido por nomeação, ter um mandato limitado e estar sujeito a supervisão de uma comissão consultiva representando as partes interessadas, incluindo representantes dos cidadãos (sociedade civil), consumidores (organizações de consumidores), responsáveis comerciais pelo tratamento (câmaras de comércio), académicos e governo e, se disponível, operadores de regimes de certificação de protecção dos dados pessoais (ver Recomendação 9, abaixo).

Os Estados-membros devem estabelecer uma DPA independente para assegurar que as leis da privacidade e da protecção dos dados pessoais estão a ser observadas. A DPA deve ter um mandato claro, poderes e recursos para poder:

- Monitorizar o cumprimento e aplicar a lei sobre a privacidade e protecção dos dados aplicável;
- Facilitar o desenvolvimento voluntário de códigos de conduta da indústria;
- Receber e resolver reclamações, petições e queixas referentes ao tratamento de dados pessoais e informar os autores das suas conclusões;
- Impor sanções e vias de recurso para contravenções à lei;
- Fazer a interpretação e, se necessário, proferir decisões vinculativas sobre a aplicação das leis;
- Avaliar sobre a adequação da protecção nas transferências de dados transfronteiriças;
- Colaborar e trocar informação, orientação e experiência das melhores práticas com DPA homólogas;
- Contactar com outros interessados (como governos, responsáveis pelo tratamento, sociedade civil) para o desenvolvimento de orientação regulamentar, quadros de confiança e medidas de habilitação como a formação das partes interessadas;
- Informar as pessoas e os responsáveis pelo tratamento dos seus direitos e obrigações;
- Desenvolver propostas para melhorar o quadro legislativo e regulamentar do tratamento de dados pessoais.

No interesse da confiança e transparência, os estados-membros devem encorajar ou exigir que as DPA, e outros organismos com responsabilidade pela monitorização da privacidade e protecção dos dados pessoais, reportem publicamente as suas actividades quando apropriado.

Pedidos de Acesso do Titular de Dados (SAR) - perspectiva das DPA

Recomendação: Os Estados-membros devem assegurar que as autoridades de protecção de dados têm os poderes apropriados relativamente aos Pedidos de Acesso do Titular de Dados (SAR), para complementar as obrigações descritas no Artigo 12º(2) da Convenção.

- Se os titulares dos dados tiverem o direito de pedir cópias dos dados pessoais a um responsável pelo tratamento de dados, as autoridades de protecção de dados (DPA) devem ser capazes de monitorizar os resultados da legislação conexa. As DPA têm poderes para assegurar que os SAR são tratados de uma forma que sirva os interesses legítimos do titular de dados, não impõe obstáculos aos titulares de dados (como taxas excessivas, procedimentos, procedimentos onerosos, etc.) e não resultam em ónus indevidos para o responsável pelo tratamento de dados.

Tema: Soluções de Várias Partes Interessadas

Esta secção faz Recomendações em diversas áreas em que resultados de sucesso dependem do esforço coordenado entre as partes interessadas.

Melhores práticas, códigos de conduta e regimes de certificação

Recomendações:

- Na busca dos objectivos de várias partes nesta secção, os Estados-membros devem convocar fóruns com várias partes interessadas incluindo as autoridades de protecção de dados, responsáveis pelo tratamento de dados e outros interessados, para complementar a base legal com códigos de conduta voluntários que implementem as melhores práticas no que se refere à privacidade e protecção dos dados pessoais.
- Governos, indústria e organismos de consumidores devem considerar a introdução de regimes de certificação para indicar que o produto ou serviço cumpre os critérios específicos para a protecção de dados. Por exemplo, a certificação pode significar que o responsável pelo tratamento de dados foi auditado face aos critérios das melhores práticas para a privacidade desde a concepção, segurança dedados ou transparência dos seus termos e condições.

Formação de uma comissão de protecção dos dados pessoais para toda a África

Recomendação: Estabelecer uma Comissão para toda a África, focada especificamente no tema da privacidade e protecção dos dados pessoais, para facilitar a coordenação e a partilha de informação entre os interessados, ajudar a identificar áreas de privacidade onde os recursos sejam necessários e aconselhar os responsáveis políticos da União Africana sobre estratégias regionais e criação de capacidade.

A Comissão seria uma rede de especialistas em evolução, compacta e de confiança formada pela CUA em colaboração com a Comunidade Africana da Internet. A liderança da Comissão deve ser cometida a múltiplas partes interessadas. Deve inspirar-se na experiência africana em geral e nas organizações nacionais e em instituições como as Comunidades Económicas Regionais (CER) e incluir DPA, empresas, representantes da academia, a comunidade técnica e a sociedade civil. Ao estruturar-se como uma rede flexível com várias partes interessadas, a Comissão pode assegurar que está posicionada para lidar com os desafios emergentes e futuros da privacidade com que a África se confronta.

A Comissão pode ficar incumbida de aconselhar e apoiar a CUA nas suas actividades relativas à privacidade ao:

- Aconselhar a CUA sobre questões e políticas de privacidade e protecção dos dados pessoais, como iniciativas de criação de capacidade;
- Ser um repositório a longo prazo para recomendações das melhores práticas sobre a privacidade e protecção dos dados pessoais;
- Identificar as áreas de investigação necessárias para formulação de políticas e directrizes gerais e específicas do sector, à medida que emergem novas circunstâncias e requisitos;
- Identificar formas para apoiar as DPA a criar capacidade e a partilhar informação ao nível regional e da União Europeia;
- Proporcionar um fórum de partes interessadas de confiança para uma divulgação responsável e coordenada das violações de dados;
- Propor formas para aumentar as competências dos profissionais da privacidade em África (por exemplo, como parte de um programa de certificação); e
- Ajudar a CUA a formular estratégias cooperativas transfronteiriças para a privacidade e criação de capacidade.

O trabalho da Comissão deve ser coordenado com a Comunicação Técnica Especializada para a Comunicação e Tecnologia de Comunicações de Informação (ICT) da UA, através dos auspícios da CUA. Detalhes referentes ao seu nome, missão, visão, objectivos e actividades detalhadas podem ser desenvolvidos pela CUA em colaboração com a Comunidade Africana da Internet.

Em particular, recomendamos esta como via para o estabelecimento da confiança através de um sistema de certificação para a protecção dos dados pessoais, com base nos conceitos descritos acima, sob "Elementos de um regime de governação". Um objectivo concreto para essa Comissão podia ser criar o quadro de confiança para pôr esse regime de coordenação em prática. O quadro definiria funções para assessores de conformidade, auditores de cumprimento e organismos de acreditação. Estes organismos, por seu turno, seriam responsáveis pelos critérios de codificação correspondentes a cada função no regime de governação.

- No caso dos responsáveis pelo tratamento e das autoridades da protecção de dados, muita dessa codificação já estaria sugerida pela legislação aplicável.
- No caso dos organismos de acreditação ou orientação referentes aos mecanismos de segurança da informação, pode ser necessário identificar ou desenvolver os critérios de avaliação relevantes.
- No caso das disciplinas de segurança da informação, os Estados-membros devem procurar fontes de orientação qualificadas, a nível nacional, regional e internacional, se necessário.

Consentimento

Recomendações:

- As autoridades da protecção de dados devem trabalhar com os responsáveis pelo tratamento de dados (por exemplo, através de organismos da indústria) para uma abordagem de colaboração com várias partes interessadas ao problema do consentimento, para acordar num equilíbrio entre medidas técnicas (como recibos de consentimento), medidas reguladoras (como avisos de cookies) e medidas de concepção do produto (como controlos e experiência do utilizador).
- Se o consentimento for legalmente qualificado (por exemplo, constrangimentos legais especificando que o consentimento deve ser informado, específico, dado de livre vontade, revogável, etc.) as autoridades da protecção de dados devem convocar um grupo de várias partes interessadas incluindo os fornecedores de serviços, advogados, sociedade civil, autores e académicos, para decidir se os requisitos são melhor cumpridos por medidas técnicas, reguladoras ou orientadas para o utilizador ou por uma combinação destas.

Finalidade da recolha

Recomendações:

- As autoridades de protecção dos dados terão de ter os poderes e os recursos necessários para aplicar o princípio da privacidade da "finalidade da recolha", conforme estipulado no Artigo 13º da Convenção. Porém, a implementação efectiva do princípio exige uma solução de colaboração e consequentemente uma abordagem por várias partes. Esta abordagem por várias partes pode e deve ser inspirada por princípios estabelecidos de privacidade desde a concepção e da privacidade predefinida, especificamente em áreas como a lealdade das decisões de concepção, minimização dos dados e respeito pela integridade contextual.
- Os governos devem assegurar que as autoridades de protecção de dados têm os recursos para monitorizar e aplicar o princípio da "finalidade da recolha". As autoridades de protecção de dados devem oferecer orientação aos fornecedores e aos prestadores de serviços sobre a necessidade de transparência e responsabilidade no que se refere a este princípio, como a base para a confiança do consumidor. Se necessário, a legislação de protecção do consumidor deve intervir para reforçar os direitos dos titulares de dados no ambiente digital.

Prazos de conservação dos dados

Recomendações:

- As autoridades de protecção de dados devem associar os responsáveis pelo tratamento (por exemplo, através dos organismos da indústria) para, em conjunto, acordarem sobre como pôr em prática o princípio do período de conservação. É provável que isto requeira uma combinação de medidas técnicas (como a definição de metadados para registar quando os dados pessoais foram recolhidos e o período decorrido o qual devem ser apagados) e as medidas regulamentares, como uma auditoria à prática do responsável pelo tratamento. [CM - Artigo 22º].
- Essas medidas de auditoria também implicam que há um organismo com recursos e capaz de realizar as auditorias. A Convenção exige que esta seja a autoridade de protecção dos dados. Os governos podem necessitar de decidir, no contexto do estado nação, se estas auditorias são realizadas numa base legal, uma abordagem baseada na gestão do risco, ou ao abrigo de códigos de conduta em sectores regulados específicos (como cuidados de saúde, serviços financeiros, etc.). [CM - Artigo 12º(2)(g)] [CM - Artigo 17º].

Tema: Bem-estar do Cidadão Digital

Expectativas dos cidadãos e dever de cuidado dos governos

Recomendações:

- Como referido acima, em "cidadãos e sociedade civil", os indivíduos abdicam em boa medida do controlo sobre os seus dados pessoais uma vez divulgados. Os responsáveis pelo tratamento arcam consequentemente com o grosso da responsabilidade de garantirem as melhores práticas e resultados de preservação da privacidade.
- Porém, os cidadãos devem tirar partido da Internet e de outras fontes de orientação para assegurar que estão adequadamente informados sobre os riscos e os benefícios das suas actividades na economia digital e no ambiente ligado, seja em casa, no trabalho ou em espaços públicos.
- Há uma função correspondente para os governos, seja directa ou indirectamente, de habilitar os indivíduos a exercer os seus direitos à privacidade, ajudando a assegurar que os cidadãos estão informados e educados sobre como exercer os seus direitos ao abrigo da lei da privacidade e da protecção de dados.
- As autoridades de supervisão e os governos devem tomar medidas para assegurar que os fornecedores de serviços online e os fornecedores de produtos são suficientemente transparentes sobre os seus modelos comerciais e as capacidades do produto, que os indivíduos estão numa posição para fazer uma escolha informada sobre as implicações de privacidade dos produtos e serviços que lhes são apresentados.

Organizações da Sociedade Civil (OSC)

Recomendações:

- Os Estados-membros devem reconhecer e apoiar o papel das OSC no:
  - Desenvolvimento de pesquisa informativa, análise, relatórios, tutoriais e materiais de defesa sobre a privacidade e a protecção dos dados pessoais para ajudar os cidadãos a compreender e a exercer os seus direitos;
  - Pesquisa das funcionalidades da privacidade e da segurança dos dados das aplicações e dos serviços em linha para identificar as boas e as más práticas; e
  - Elaboração de análises independentes, objetivas e baseadas na prova do "estado da privacidade e da protecção dos dados", como função de monitorização para proteger e representar os interesses dos indivíduos.
- Os Estados-membros são encorajados a considerar as OSC como parceiras na criação de uma população segura, conhecedora e capaz de "cidadãos digitais" e devem assegurar que as OSC têm o quadro e as protecções legais no âmbito das quais contribuem para esta parceria.

Tema: Habilitação e Medidas de Apoio

O Artigo 31º da Declaração Ministerial (Adis Abeba, Novembro de 2017) recorre à CUA "para assegurar que é dado seguimento à assinatura e ratificação pelos Estados-membros" da Convenção de Malabo.

Em conformidade, encorajamos os Estados-membros a adoptarem a seguinte abordagem, tendo em vista acelerar e aumentar a confiança para que os membros sejam capazes de adoptar e implementar as medidas exigidas pela Convenção.

Recomendações: Os Responsáveis Políticos devem colaborar com Sociedade Civil, defensores da privacidade, empresas, académicos e outras partes interessadas na criação de materiais de formação e explicativos sobre os seguintes tópicos. O objectivo destes materiais seria ultrapassar as barreiras representadas pela falta de sensibilização, conhecimento e compreensão.

- Fundamentos da privacidade digital e dos seus riscos e benefícios
- Modelos comerciais comuns e/ou dominantes para os serviços online
- Publicidade e monetização de dados numa economia orientada pelos dados

- Sensibilização para as diferentes culturas e expectativas de privacidade no e para além do contexto africano
- Privacidade desde a Concepção e a perspectiva de tecnologias de melhoria da privacidade
- Inclusão/exclusão digital e partes interessadas marginalizadas
- Riscos e prejuízos que podem decorrer de actividades online e de modelos comerciais orientados pelos dados
- Implicações das tecnologias emergentes (data mining, aprendizagem da máquina e Inteligência Artificial; sistemas autónomos; Internet of Things, etc.)
- ... E quaisquer outros tópicos que ocasionalmente se venham a tornar relevantes

Estes materiais devem constituir a base de um programa de mesas redondas de partes interessadas, incluindo a participação de responsáveis políticos, cujo objectivo é capitalizar no conhecimento e sensibilização obtidos e colocá-lo imediatamente em prática sob a forma de envolvimento renovado das partes interessadas. O programa deve ter os seguintes objectivos:

- Troca de informação e estabelecimento da confiança entre partes interessadas ao nível político, técnico, jurídico, empresarial, académico e da sociedade civil;
- Aumentar o conhecimento, sensibilização e confiança dos responsáveis políticos nestes tópicos;
- Assegurar que os responsáveis políticos têm oportunidade de colocar esse conhecimento em prática junto das suas comunidades de partes interessadas; e
- Dar uma voz às partes interessadas informadas e interessadas na moldagem do futuro online dos seus países, regiões e continente.

Os membros podem considerar inspirar-se para esse programa na abordagem relativa à cibersegurança exigida pelo Artigo 31º da Declaração de Adis Abeba (AU/CCICT-2), que prevê uma conferência anual sobre cibersegurança e um mês de cibersegurança transversal ao continente.

Por exemplo, pode ser produtivo instituir um agendamento regular de:

- Publicação de um dos materiais de formação indicados acima;
- Um período para leitura e reflexão; e
- Uma workshop sob a forma de mesa redonda das partes interessadas para discutir o tópico e acordar nas ações resultantes.

Estas actividades podem culminar numa conferência anual e num mês focado na protecção de dados e na privacidade em linha..

Sobre a Internet Society

A Internet Society (ISOC) apoia e promove o desenvolvimento da Internet como uma infra-estrutura técnica global, um recurso para enriquecer a vida das pessoas e uma força para o bem na sociedade. Trabalhando através de uma comunidade global de associações e membros, a Internet Society colabora com um vasto número de grupos na promoção das tecnologias que mantêm a Internet segura e defende políticas que possibilitem o acesso universal.

Juntos, focamo-nos no:

- Estabelecimento e apoio às comunidades que fazem a Internet funcionar;
- Avanço do desenvolvimento e aplicação das infra-estruturas, tecnologias e padrões abertos da Internet;
- Defesa de uma política que seja consistente com a nossa visão da Internet.

Sobre a Comissão da União Africana

A União Africana (UA) foi lançada oficialmente em Julho de 2002, no seguimento de uma decisão em Setembro de 1999 da sua predecessora, a Organização de Unidade Africana (OUA), que tinha sido constituída em 1963, visando criar uma nova organização continental para desenvolver o seu trabalho. Um total de 54 países juntaram-se à nova organização, cuja sede permaneceu em Adis Abeba, Etiópia.

A Comissão da União Abricana (CUA) é o secretariado da UA, à qual cabe o poder executivo. É composta por 10 membros, um Presidente, um Vice-presidente e 8 Comissários. A estrutura representa a UA e protege os seus interesses sob os auspícios da Conferência de Chefes de Estado e de Governo, bem como do Conselho Executivo.

A CUA é responsável pelas seguintes pastas: Paz e Segurança, Assuntos Políticos, Comércio e Indústria, Infra-Estruturas e Energia, Assuntos Sociais, Economia Rural e Agricultura, Recursos Humanos, Ciência e Tecnologia e Assuntos Económicos.

A visão orientadora para a Agenda 2063 é a visão da UA de: "Uma África integrada, próspera e pacífica, dirigida pelos seus próprios cidadãos e representando uma força dinâmica na arena global". A missão da Comissão da UA é "tornar-se uma instituição eficiente e com valor acrescentado que conduz a integração de África e o processo de desenvolvimento em estreita colaboração com os Estados-membros da União Africana, as comunidades económicas regionais e os cidadãos africanos".