CONSCIOUS YOUTH BEHAVIOURS
IN EMERGING REALITIES

Práticas de educação não-formal:

Morphing e Deepfakes

R2 CYBER TOOLKIT

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

#13	**Dominar o Enigma Digital: Neutralizar os Fenómenos Morphing e Deepfake**
Ameaça(s)	**Morphing e Deepfakes**
	O morphing envolve a manipulação de imagens digitais, com recurso a ferramentas online, possibilitando aos infratores adulterar fotografias publicadas online para fins ilícitos, frequentemente visando raparigas e mulheres jovens. Estas imagens alteradas podem ser utilizadas como chantagem, para a criação de perfis fictícios online, sexting, conversas sexuais ilícitas e produção de conteúdos pornográficos. Os ataques de morphing podem envolver a utilização de software de edição de imagem para combinar fotografias biométricas de passaportes, produzindo uma imagem que representa, de forma enganadora, uma combinação de dois indivíduos. Do mesmo modo, os deepfakes representam uma forma sofisticada de manipulação digital, em que a aparência de alguém numa imagem ou vídeo é substituída pela de outra pessoa, criando conteúdos altamente realistas, mas inteiramente falsificados. Os deepfakes acarretam riscos significativos na esfera das ciberameaças aos jovens, uma vez que contribuem para a disseminação da desinformação, manipulam perceções e facilitam o ciberbullying, ampliando assim o potencial de perigo e aproveitamento no domínio digital.
Tipologia	Análise crítica do conteúdo online
Duração	120 minutos/2 horas (pode ser adaptado em função da intensidade das atividades)
Modalidade	Presencialmente [contexto de sala de aula]
Finalidade	A finalidade desta prática é dotar os participantes das competências e conhecimento necessários para avaliarem criteriosamente imagens e vídeos digitais, efetuarem juízos de valor ao interagirem com conteúdos “morphed” ou “deepfake”, adotarem um comportamento responsável online e protegerem a sua identidade digital pessoal.
Objetivos de aprendizagem	Avaliar de Forma Crítica Imagens Digitais: Os participantes são capazes de examinar criticamente imagens digitais para detetar indícios de manipulação, recorrendo à sua compreensão das técnicas de morphing. Aplicar Juízos Éticos: Os participantes demonstram a capacidade de aplicar juízos éticos ao criar, partilhar ou serem confrontados com imagens modificadas, reconhecendo os potenciais danos e respeitando os direitos dos indivíduos. Demonstrar um Comportamento Responsável Online: Os participantes demonstram um comportamento responsável online ao respeitar a privacidade, obter consentimento prévio à partilha de imagens e desencorajar a disseminação de informações falsas através de imagens modificadas. Proteger a Identidade Digital Pessoal: Os participantes implementam estratégias eficazes para proteger imagens e informações pessoais online, nomeadamente definições de privacidade fortes, a inserção de marcas de água em fotografias pessoais e a prudência na partilha de imagens nas redes sociais.

Perfil dos formandos	Faixa Etária: 15-17 anos Formação Escolar: Estudantes do ensino secundário Pré-requisitos: Conhecimento básico de navegação na Internet e nas plataformas de redes sociais
n° de participantes	15-20 (ideal para dinamizar discussões e atividades de grupo)
Materiais	Dispositivos com acesso à Internet (computadores portáteis/tablets) Projetor e ecrã para apresentações Quadro branco e marcadores Folhetos impressos com exemplos de imagens/vídeos morphed e deepfake Guias e recursos para a verificação de factos Cadernos e canetas para os participantes
Preparação	Preparar o Local: Dispor os assentos da sala de aula de forma a facilitar as discussões em grupo e a visualização do ecrã do projetor. Preparar os Materiais: Assegurar que todos os dispositivos digitais se encontram ligados à Internet e pré-carregar websites e exemplos relevantes. Imprimir os folhetos e garantir que todos os materiais se encontram disponíveis.
Implementação	*Introdução (10 minutos):* Acolher os participantes e introduzir o tema. Explicar sucintamente as ameaças resultantes do morphing e deepfakes. Delinear os objetivos e a estrutura da sessão (opcional). *Apresentação Interativa (30 minutos):* Apresentar exemplos de conteúdos “morphed” e “deepfake”. Os exemplos são facultados no Anexo_. Discutir as técnicas empregues na criação destes conteúdos. Sublinhar as repercussões no mundo real e as questões éticas. *Atividade de Grupo: Análise Crítica (30 minutos):* Dividir os participantes em pequenos grupos (3-4 pessoas). Fornecer a cada grupo um conjunto de imagens e vídeos digitais. Existem muitos disponíveis online. Convidar os grupos a identificar sinais de manipulação e a discutir as suas conclusões.

	Juízos Éticos e Comportamento Responsável (20 minutos): Facilitar uma discussão em grupo acerca das implicações éticas do morphing e dos deepfakes. Incentivar os participantes a partilhar as suas perspetivas sobre o comportamento responsável online. Apresentar casos reais em que o morphing e os deepfakes causaram danos. *Proteção da Identidade Digital Pessoal (20 minutos):* Partilhar estratégias para salvaguardar imagens e informações pessoais online. Demonstrar como aplicar definições de privacidade e utilizar ferramentas de marca de água. Discutir as melhores práticas para a partilha de imagens nas redes sociais. *Q&A e Conclusão (10 minutos):* Abrir espaço para perguntas e respostas. Resumir as principais conclusões da sessão. Fornecer recursos complementares para aprendizagem adicional (opcional).
Dicas e sugestões	Estimular a participação ativa, formulando questões abertas e promovendo o debate. Recorrer eficazmente a recursos visuais para ilustrar argumentos e manter os participantes envolvidos. Utilizar uma variedade de exemplos, incluindo casos simples e complexos de morphing e deepfakes, para atender a diferentes níveis de compreensão.
Medidas de segurança	Assegurar a segurança na Internet durante as atividades online. Estabelecer um espaço de debate respeitador e sem preconceitos.
Valor acrescido	Os participantes adquirem a capacidade de identificar conteúdos manipulados, compreender as implicações éticas da criação e partilha de conteúdos manipulados, o que lhes permite adotar um comportamento online mais responsável, reduzir o risco de utilização inadequada, reforçar a sua privacidade online e desenvolver o espírito crítico.
Feedback e avaliação	Encorajar os participantes a transmitirem feedback no final da sessão, com vista a otimizar atividades futuras.
Conclusão	Esta prática aborda, de forma eficaz, as ameaças emergentes resultantes do morphing e deepfakes, fornecendo aos participantes competências e conhecimentos fundamentais. A prática reforça não só a literacia digital, como

	também promove o comportamento responsável e o pensamento crítico, enquadrando-se perfeitamente com os objetivos estabelecidos. Os participantes terminam com uma maior consciência da manipulação digital e das ferramentas para a combater, o que torna esta prática altamente relevante e impactante na era digital contemporânea.

Anexo. Material para Imprimir de exemplos Populares de Morphing e Deepfake

Exemplo Popular de Morphing
FaceApp e Filtros do Snapchat: Estas aplicações populares permitem aos utilizadores trocar de rosto com celebridades ou outros indivíduos. Os utilizadores podem capturar uma fotografia e utilizar as ferramentas da aplicação para sobrepor o rosto de uma celebridade ao seu próprio rosto, criando imagens divertidas ou sinistras. Por exemplo, as pessoas costumam combinar os seus rostos com atores como Leonardo DiCaprio ou cantoras como a Beyoncé para observar como seria o seu aspeto como personalidades famosas.
Exemplos Populares de Deepfake
The Mandalorian (Série Star Wars): A personagem de Luke Skywalker, conforme surgiu nos anos 80, foi recriada a partir de tecnologia deepfake, na série Star Wars "The Mandalorian". Isto permitiu que a personagem aparentasse ser bem mais jovem do que a idade real do ator.

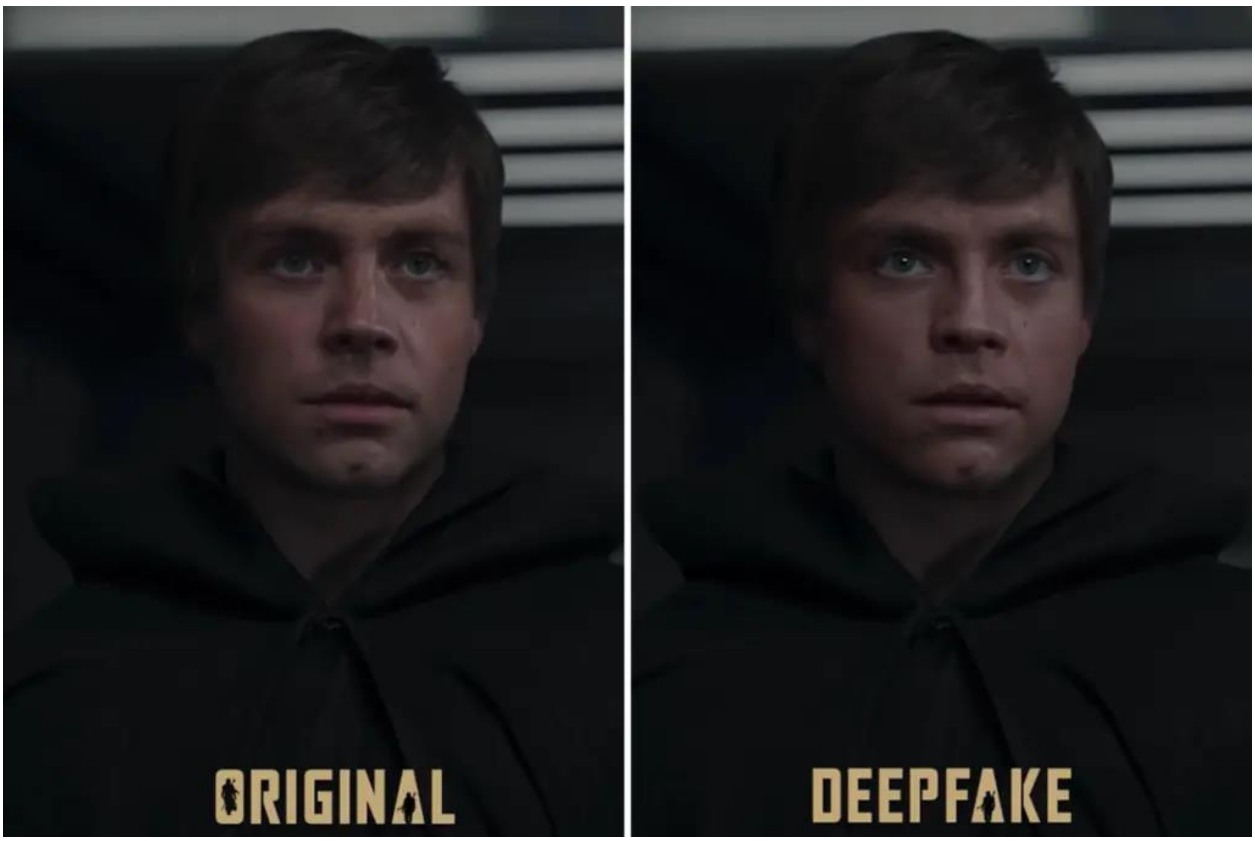
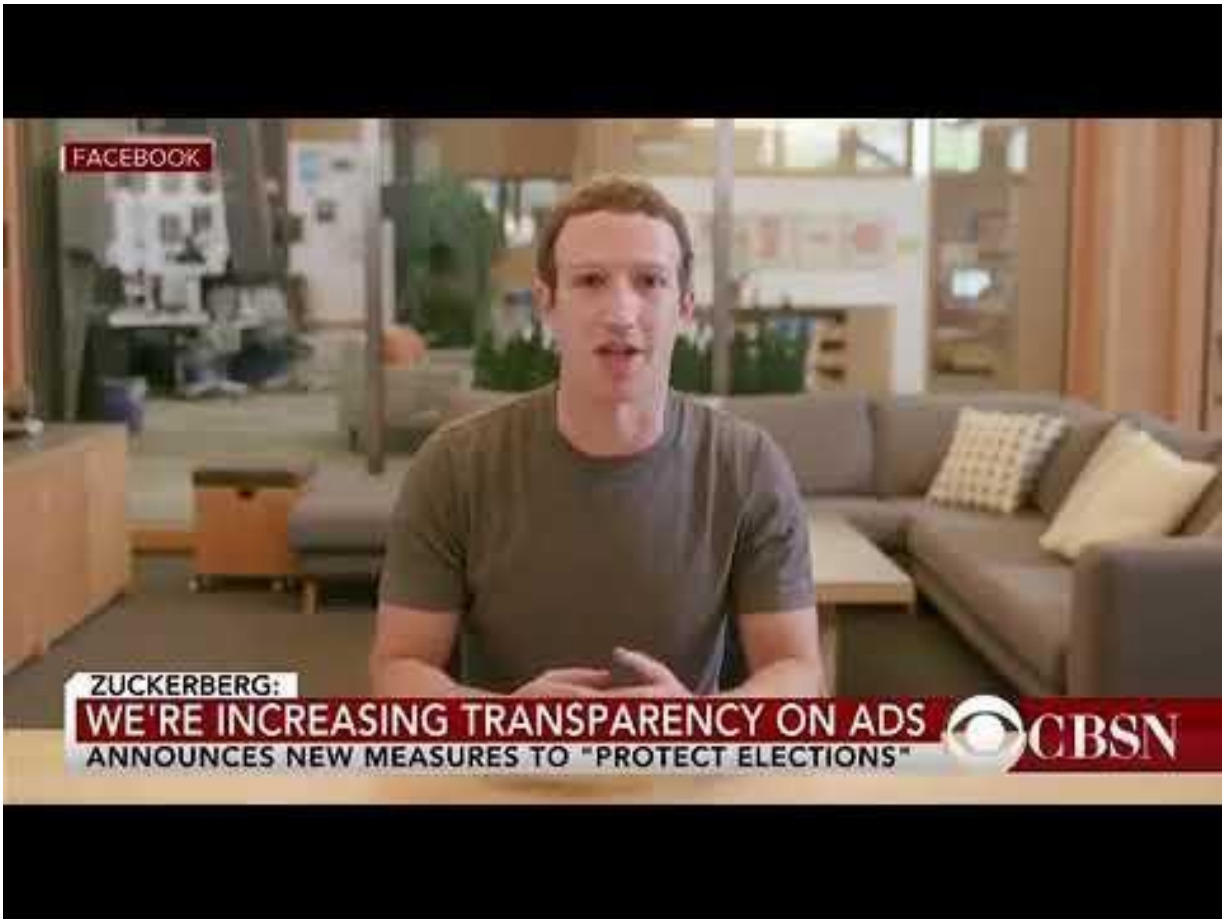


Figura 1: The Mandalorian (Série Star Wars): O Deepfake da personagem de Luke Skywalker (Fonte: https://nypost.com/2022/02/03/fans-suspect-youtuber-behind-awesome-book-of-boba-fett-cgi/)

Deepfake de Mark Zuckerberg: Um vídeo do CEO do Facebook, Mark Zuckerberg, em que aparentemente discute o controlo de mil milhões de dados pessoais roubados. Este deepfake foi criado como um projeto artístico para realçar as preocupações com a privacidade e o eventual uso indevido da tecnologia deepfake.



Anexo. Técnicas Empregues na Criação de Conteúdo de Morphing e Deepfake

Durante o segmento de apresentação interativa, o facilitador deve abordar as seguintes técnicas empregues na criação de conteúdos morphed e deepfake:

Modificação de Imagem:

Edição Manual: Recorrer a um software, como o Adobe Photoshop, para editar manualmente as imagens, combinando elementos de várias fotografias. Isto inclui técnicas como a sobreposição, a ocultação e os modos de mistura.

Substituição de rosto: Usar ferramentas e aplicações de troca de rostos que substituem de forma automática o rosto de uma pessoa pelo de outra numa fotografia ou vídeo.

Ferramentas assistidas por IA: Utilizar ferramentas de IA que permitem modificar rostos através da interpretação das estruturas faciais e efetuar modificações realistas.

Criação de um Deepfake: **Redes Generativas Adversárias (GANs):** Compreender como operam as GANs, com uma rede neural a gerar imagens falsas e outra a tentar detetá-las, refinando as falsificações ao longo do tempo. **Autocodificadores:** Utilizar autocodificadores, que são redes neuronais programadas para comprimir imagens e depois reconstruí-las, a fim de modificar os rostos nos vídeos, associando-os a um rosto diferente. **Algoritmos de Aprendizagem Avançada:** Aplicação de algoritmos de aprendizagem avançada para criar vídeos fictícios altamente realistas, praticando em vastos conjuntos de dados de imagens e vídeos da pessoa-alvo. **Síntese de Fala:** Uso de tecnologias de conversão de texto em voz e modelos de aprendizagem avançada para clonar a voz de um indivíduo, tornando o deepfake ainda mais credível devido à sincronização da voz com o vídeo.
Edição de Vídeo: **Edição quadro a quadro:** Edição manual de quadros de vídeo para alterar aparências ou ações, o que consome muito tempo, mas produz manipulações deveras detalhadas. **Rastreio do movimento:** Utilização de software para rastrear e manipular o movimento de elementos num vídeo, garantindo que as alterações possuem um aspeto natural à medida que o motivo se desloca. **Sincronização Labial:** Uso de tecnologias de sincronização labial para fazer corresponder os movimentos da boca de alguém no vídeo a uma faixa de áudio distinta, frequentemente aplicada juntamente com a síntese de fala.

Conscious Youth Behaviours in Emerging Realities

Erasmus+ KA2 Cooperation Partnerships in School Education

[Reference n. 2023-1-EL01-KA220-SCH-000156982]

Co-funded by the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.