ORIGINAL RESEARCH

The ethics of computer vision: an overview in terms of power

Rosalie A. Waelen[1] (ORCID)

Abstract
Computer vision is a subfield of artificial intelligence, aimed at making computers see. Computer vision tools enable a system or device to automatically analyze, interpret, and respond to images and videos. Computer vision tasks range from object detection and tracking, to the recognition of people's faces and emotional states. While the ethics of AI in general has received significant attention, and the ethics of facial recognition (a computer vision application) too, little of the AI ethics literature focuses specifically on the ethics of computer vision. In this chapter, I create an overview of ethical, social, and political issues related to computer vision, using a critical approach. This means that I identify issues in terms of power and evaluate them in function of their impact on the value of autonomy and the normative goal of emancipatory progress. The aim of this chapter is first and foremost to offer an overview of potential normative implications of computer vision. Additionally, the chapter functions as an example for the use of a critical approach to AI ethics.

Keywords Computer vision · Video analytics · Facial recognition · AI ethics · Power

1 Introduction

Computer vision (CV) involves the use of artificial intelligence (AI) techniques to automate the analysis of images and videos. CV comprises several tasks, including tracking, identification, detection, classification, localization, segmentation, facial recognition, emotion recognition, and behavior recognition. These tasks can serve a wide variety of purposes: from reading handwritten texts to recognizing traffic signs, and from interpreting MRI-scans to sentiment analysis of audiences. Given the many possible use cases of computer vision, it is easy to imagine that the technology can significantly impact everyday life and societal practices. This article provides an overview of the potential ethical, social, and political implications of CV. The overview focuses on those CV applications that analyze the visual data of human persons. The method used to create the overview is a critical approach, based on a pluralistic understanding of power (as proposed by Waelen [25]).

The outline of the article is as follows. In Sect. 2, I discuss related work on the ethics of CV. In Sect. 3, I introduce the critical approach used to analyze CV's potential normative implications. In Sects. 4, 5, 6 and 7, I apply the approach to identify and evaluate the issues in CV related to dispositional power, episodic power, systemic power, and constitutive power. I end the chapter with a conclusion in Sect. 8.

2 Related work

A quick narrative review of the AI ethics literature shows that there is little work on the ethics of CV, despite the widespread attention for AI ethics and the importance of CV within AI research.

For starters, in general discussions of AI ethics, CV and its different applications are hardly mentioned.[1] The *Stanford Encyclopedia of Philosophy* entry on 'Ethics of Artificial Intelligence and Robotics' [20] and the *Internet Encyclopedia of Philosophy* entry on 'Ethics of Artificial Intelligence' [11] both only refer to facial recognition once and do not explicitly mention CV at all. In *The Oxford Handbook of Ethics of AI* [9], there is not a single chapter dedicated to CV or CV applications—although CV applications are among the examples discussed in some of the chapters. In Mark Coeckelbergh's book *AI Ethics* [4], computer vision is briefly mentioned as one of many AI techniques and facial

✉ Rosalie A. Waelen
   r.a.waelen@utwente.nl

1   Section of Philosophy, University of Twente, Enschede, The Netherlands

---

[1] The same could be said for Natural Language Processing (NLP), which is another main subfield of AI.

recognition repeatedly pops up in examples (regarding surveillance and privacy, data and biases, Walmart's analysis of customers, and Facebook's photo tagging), but neither the technology nor the examples are discussed with much detail. In Kate Crawford's book *The Atlas of AI. Power, Politics, and the Planetary Cost of Artificial Intelligence* one can find more detailed discussions of CV—although still only in relation to examples that are meant to portray other issues. The discussion of CV in Crawford's book shows a lot of overlap with her essay on the normative issues in CV research that was published on the webpage *excavating.ai* [7]. For instance, she discusses the enormous amount of energy needed to store the big datasets needed to develop CV models, the problematic assumption that images are apolitical and can be given a single label, and the problems with Ekman's theory of the facial expressions of emotions on which most CV-based emotion recognition models build.

However, despite the lack of attention for CV in general works on AI ethics, there are some focused articles dealing explicitly and exclusively with the ethics of CV or certain CV applications. Already in 2004, Brey discussed the ethics of the use of facial recognition in public spaces. He highlights the problem of error, the problem of function creep, and privacy—noting that the latter is the most serious obstacle to facial recognition applications in public space [2]. Selinger and Leong [22] wrote a chapter on the ethics of facial recognition in *The Oxford Handbook of Digital Ethics*, discussing among other things the uniqueness of facial recognition technology. In their much-cited paper 'Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification' [3], Buolamwini and Gebru discuss algorithmic fairness in the context of facial analysis systems that classify a person's gender based on the image of their face. Thiago Guimarães Moraes and colleagues discuss different purposes in which facial recognition is used in (semi-)public spaces in Brazil (namely for public security, social scoring and digital identity, private security, targeted marketing, and public health) and the risks that come with these applications (the lack of a legal basis, inaccuracy, normalization of surveillance, and a lack of transparency) [18]. Blank et al. analyze the ethics of facial recognition in general. Although they claim to build on various approaches in AI ethics, such as the expansion of bioethics into AI suggested by the AI4People framework, they end up focusing on three issues—human rights, error rates, and bias—without explaining why these would be the most important to discuss [1].

There are also a number of focused articles on aspects of CV other than face recognition or facial analysis. Crawford's aforementioned piece on *excavating.ai* offers an in-depth discussion of the problems surrounding ImageNet—the main database used in CV research. Coupland et al. discuss how ethical consideration could or should be part of the development of CV applications, on the basis of a specific case study—namely, a CV system for person tracking, occupancy and fall detection [5]. Huffer et al. go into the ethics of CV in the context of human remains trafficking [14]. Dufresne-Camaro et al. wrote a paper on CV research for the global South and the risks related to the uses of CV in the global South. They find that the focus of CV research is different in the global South and the risks related to CV applications and uses are "region-specific, depending heavily on a community's needs, norms, culture and resources" [10, p. 8]. In a report for the American Civil Liberties Union, Stanley [24] discusses the dangers of AI cameras and video analytics. Although Stanley's report focuses solely on the use of CV for surveillance, it covers a fairly wide range of ethical issues—including chilling effects, the new types of data smart cameras can gather, the unscientific basis of certain forms of analytics, discriminatory effects, and the possibility of over-enforcement and abuse of the technology.

To the best of my knowledge, only two sources cover the ethics of CV in general, rather than focusing on a specific application or use context. The first source is a Master's thesis, in which six ethical themes in computer vision are identified on the basis of a literature review: espionage, identity theft, malicious attacks, copyright infringement, discrimination, and misinformation [15]. The second piece on the ethics of CV is a conference paper by Skirpan and Yeh, titled 'Designing a Moral Compass for the Future of Computer Vision using Speculative Analysis'. The authors categorize five risks in CV: privacy violations, discrimination, security breaches, spoofing and adversarial inputs, and psychological harms [23].

Computer vision research covers a huge part of AI research and the developments in AI over the past decade started with a breakthrough in CV research [17]. When it comes to AI ethics, however, CV is much less central. Admittedly, the topic is not entirely ignored, and facial recognition has even become one of the most discussed topics in AI ethics. But on the basis of this brief literature review, I conclude that a comprehensive overview of potential ethical, social, and political issues in CV would nevertheless be a valuable addition to the AI ethics literature.

3 Method

To create an overview of CV's ethical, social, and political implications (CV's normative implications, for short), I opt for a critical approach (as proposed by Waelen [25]). The critical approach is inspired by the tradition of critical theory, which focuses on critiquing power dynamics and has the practical aim of realizing emancipatory progress. The critical approach has multiple benefits: it covers not only strictly ethical issues, but also social and

Table 1 Dispositional power

How can CV disempower people?	How could this affect autonomy and emancipatory progress?
Less informational control	Challenges ability to own one's life story
Less anonymity	Challenges ability to act and develop independently
Less epistemic agency due to technical and legal complexities surrounding CV practices	Challenges ability to follow one's own judgment and potentially harms self-development
Less testimonial agency due to automated interpretation of identity	Challenges ability to own one's life story
Less acting out of moral duty due to possibility of over-enforcement using CV	Challenges ability to follow one's own moral judgment and develop one's own moral reasoning
Loss of important skills due to dependency on CV applications	Challenges ability to follow one's own judgment

political implications; it avoids abstract ethical terminology; and it has a clear normative goal, namely furthering emancipatory progress. Ethical, social, and political implications of CV are identified and evaluated using a power framework. The power framework is based on a pluralistic understanding of the concept of power [13, 21, 25].

Haugaard [13] has argued that one should treat power as a family resemblance concept. This entails that different definitions of power that are usually taken to be opposing views, are treated as different aspects of the same thing and therefore as complementary views of power. Each aspect of power that is included in the framework, is included because it is useful for understanding the ways in which AI applications like CV might threaten or compromise human autonomy and emancipatory progress. The four aspects of power that make up the framework for the analysis are (1) *dispositional power*, or the potential to bring about significant outcomes; (2) *episodic power*, or the exercise of power by A over B, which makes B act differently than they otherwise would have; (3) *systemic power*, or the dominant laws, norms and practices in a society; and (4) *constitutive power*, or the ways in which power shapes a person's identity, thoughts and behavior [13, 21].

In what follows I devote a separate section to each of these four aspects of power. In each section I identify potential normative issues related to the respective form of power. I evaluate the identified issues by discussing their impact on autonomy and, consequently, emancipatory progress in society. For the purposes of this paper, I understand autonomy as the ability to follow one's own judgment (self-legislation) and the ability to develop and own one's life story (self-ownership). People form their own judgment and their life story in relation to and communication with others. The focus of the chapter lies predominantly on applications that analyze images or videos of persons. Furthermore, it should be noted that CV can also impact people and emancipation in a positive way.

However, the present analysis focuses only on the potentially problematic impact of CV.

4 Dispositional power

Let us start the analysis with the dispositional view of power. This view, quite obviously, holds that power is a disposition or ability. However, one should not think of every human disposition or ability in terms of power. Dispositional power is the ability to bring about significant outcomes [19]. People are empowered when they gain dispositional power and disempowered when they lose it. When an individual or group is empowered or disempowered, their scope of agency increases or decreases. More agency promotes autonomy, it namely means that people are better able to act as they see fit, to develop themselves, and to explore opportunities. So, empowerment is a good worth striving for and disempowerment an ethical problem. When considering ethical and other normative issues in CV, it is therefore worthwhile asking: How can CV empower or disempower individuals? And: Do CV's disempowering effects limit people's autonomy? In this section, I identify six ways in which CV applications could potentially disempower people and discuss how these forms of disempowerment relate to autonomy (as defined above). The findings are summarized in Table 1 at the end of the section.

First of all, like many other modern technologies, CV limits people's informational control. CV applications retrieve information about individuals from visual data that is either pre-existing footage or gathered in real-time (e.g. through a camera on a personal device or a CCTV camera in a public place). When dealing with stored, pre-existing visual data, the persons displayed on the image or video (as well as the people taking the footage) most likely did not know that the footage would later be used as input for CV applications. In the case of real-time recordings, it can be difficult for a person to avoid being

recorded, because that would mean they could not freely move in public places or could not use certain devices or applications. So, in both cases, CV seriously challenges people's ability to consent to their data being gathered and analyzed. On top of that comes the fact that it is particularly difficult to hide or protect one's data from CV tools, because it is people's appearance that is revealing information in this case. For example, video analytics systems analyze a person's facial expressions or the way they walk. Protecting one's information, in this context, would imply taking extensive measures, such as hiding one's face or changing the way one dresses.

These threats to informational control can be understood as disempowering. Less informational control harms autonomy, because it limits an important ability: the ability of a person to decide who knows what about them. This ability is an element of self-ownership. Understanding informational control in terms of disempowerment also enables us to see how the concern for informational control, being a concern for privacy, derives from a more fundamental concern for human emancipation. People do not value informational control for its own sake, but because it promotes their autonomy.

Secondly, related to the loss of informational control is a diminishing ability to go places anonymously. Anonymity is not just something that benefits criminals or people with bad intentions, anonymity helps people to "feel freer to associate with whomever they want, read and watch what they choose, and express their opinions as they see fit" ([8], p. 210). In other words, anonymity creates the safe space that people sometimes need to act as they wish to and develop themselves. For example, public anonymity allows a person to visit a LGBTQ bar or attend a political protest, without their friends, family, or colleagues being able to find out. Anonymity also safeguards those fleeing oppressive regimes or those who, for good reasons, had to take on a new identity. So being able to go places anonymously is empowering in that it promotes the ability to act and develop freely and independently. A threat to anonymity is therefore also a threat to autonomy.

Thirdly, CV can decrease people's epistemic agency. Not only does CV challenge the extent to which people control what data is gathered and what is known about them, advanced data analysis also makes it increasingly difficult for the average individual to grasp what information is or could be retrieved from visual data. A person might therefore not know what information may be revealed when they are filmed by a 'smart camera' (as CV supported cameras are often called) or when they share images of themselves online. Furthermore, in addition to the technical complexity, there is also complexity regarding what data can legally be gathered and shared with third parties. This additional layer of complexity, or illiteracy, contributes to the loss of epistemic agency that CV applications can cause. A loss of

epistemic agency due to the technical and legal complexity of CV applications relates to dispositional power in that it implies a decline in people's ability to follow their own judgment. Since I understood self-legislation as an important element of autonomy, I conclude that CV's effect on epistemic agency can threaten autonomy. Furthermore, the feeling of lacking sufficient epistemic agency to navigate the technical world around oneself, might also impact a person's self-confidence. Such an impact can also be understood as limiting autonomy, harming self-development namely implies harming a person's identity development.

Fourth, people lose testimonial agency when CV systems deprive them of the opportunity to communicate who they are and how they feel. Some CV applications automatically infer people's identity, demographic information, mood, or other characteristics. As a result, people are no longer able to communicate this information themselves. The ability to communicate one's own identity is important, not only because it allows people to control how much is known about them, but also because it enables them to shape their identity and exercise control over how they are perceived and treated by the world around them. In other words, testimonial agency supports the ability to own one's life story and thus supports autonomy. The way people present themselves is not objective: they stress the characteristics that they find most important and leave out those that they do not want others to know about of or associate them with. Maybe a person strongly identifies with a specific characteristic, such as their religion or ethnicity. Or conversely, maybe a person prefers to hide a certain characteristic, because they want to avoid being treated in discriminatory or stereotypical ways. CV tools could infer objective facts about people, such as their age and gender, but they cannot read from one's face what their subjective sense of identity is or who they aspire to be.

Fifth, CV might also affect people's ability to act out of moral duty. Hale [12] develops this idea in his 'subjective freedom argument' against face recognition technology. Hale argues that facial recognition will enable law-enforcement to become (close to) complete—meaning that every deviation from the law, every small wrongdoing (think jaywalking or littering), can be detected and penalized. Hale explains that such over-enforcement would be a moral problem, because moral behavior would no longer stem from people's own moral reasoning or inner moral laws, but only be the result of people's awareness that they are being watched and will be penalized if they do not act according to society's laws. Without a need to act out of duty, following one's own moral reasoning, citizens do not get the opportunity to develop their moral autonomy. In other words, CV could diminish people's ability to follow as well as people's ability to develop their own moral judgment. Of course traditional video surveillance could affect moral autonomy too, but

CV automated surveillance would make law-enforcement that much more effective that the impact on moral autonomy could be more significant too.

Finally, there are risks related to depending too much on a technology. The use of CV applications can result in deskilling, i.e., the loss of important human skills. This would for example be the case when people learn to depend on facial recognition systems to identify people or read their emotions, and thereby forget how to remember names and faces and interpret facial expressions. Or when people depend solely on photo translator applications when finding their way in a foreign country. Dependency or reliance on technology can be disempowering. Such disempowerment is problematic to the extent that it prevents a person from following their own judgment (self-legislation) or forming their own life story (self-ownership). Particularly in the example of deskilling one could argue that self-legislation is at stake.

5 Episodic power

The term 'episodic power' refers to the exercise of power by one actor over another. This view of power is therefore also often referred to as 'power-over'. One has power over another when they get them to act or think in a way they otherwise would not have acted or thought. Technology can facilitate the exercise of power "by either giving them new powers or by improving the efficiency, effectiveness, reliability and ease by which existing powers are exercised [2, p. 81]. So CV applications can function as tools that enable the exercise of power, but they can also simply add force to power that would have been exercised anyway. This is not necessarily bad news. Power relations are not always problematic they are an unavoidable part of life (think of parents having power over their children, or employers having power over their employees). In line with critical theory's emancipatory aim, we can say that episodic power becomes a moral concern when an exercise of power significantly compromises a person's self-legislation and self-ownership. Hence, the impact of a power relation on autonomy needs to be proportional to be morally acceptable.

A big part of CV's use for the exercise of power lies in its potential to automate surveillance. Surveillance makes it possible to control the way people act, either by detecting or punishing it when people act wrongly, or because people act differently when they are aware of being monitored. Before, camera surveillance depended on human operators to monitor video footage. Now that the monitoring of video footage is automated by CV, camera surveillance can be implemented on a much wider scale. As a consequence, surveillance also emerges in new contexts—take for example parents surveilling their children, health providers

surveilling elderly or sick people in their homes, or insurance companies surveilling drivers in their cars. CV's automation of surveillance therefore facilitates the exercise of power by many parties: by law enforcement and security, by insurance companies, by employers, by private persons, and more.

As already pointed out in the previous section, CV enabled surveillance could lead to over-enforcement. By automatically detecting every single instance of misbehavior, however small, law enforcement could become too restrictive. While it is still enforcement of the law, which in itself is not problematic according to most people, over-enforcement could make the power law has over citizens too restrictive of people's freedom to act as they see fit (hence, their self-legislation).

CV enabled surveillance by insurance companies strengthens the power of insurance companies over individuals' behavior. There naturally is a power relation between these two parties, but the power relation becomes (much) more asymmetric when insurance providers are able to surveille clients. This raises the question: how much power do we want insurance companies to have over people's behavior? Take the example of video surveillance inside a person's vehicle, aimed at judging a person's driving style. Just like it seems sensible that law enforcement uses its power to make people obey the law, it also seems sensible that insurance companies take efforts to stimulate safe driving. While most people would agree that one should obey the law and drive safely, it still seems wrong to be forced to do so. As already pointed out in the previous section, respecting autonomy requires giving people the freedom to develop and follow their own (moral) judgment.

In the case of workplace surveillance by employers over employees, a similar issue arises. CV also enables employers to automatically surveille employees. Depending on the work environment, workplace surveillance can entail detecting certain behaviors like chatting with co-workers or smiling to customers, or taking record of the time spent on specific tasks or at a desk. Again, it seems sensible for employers to see to it that their employees do their job as they should. However, using the power of CV automated surveillance to get employees to behave as expected, employers violate the ability of employees to follow their own judgment and do well at their job out of their own volition. Moreover, workspace surveillance signals distrust to employees, which can negatively affect their relationship to their employer and the joy or pride employees experience in doing their job.

CV also makes camera security more affordable for private persons and enables new kinds of products, such as systems that monitor baby-rooms and warn the parents when the child wakes up or tries to climb out of their bed; systems that detect when elderly people fall inside their homes and automatically

Table 2 Episodic power

How can CV facilitate the exercise of power?	Does this instance of power affect autonomy?
Stricter enforcement of the law through automated camera surveillance	Challenges ability/freedom to develop and follow one's own (moral) judgment
Disproportional power of insurers over clients due to use of automated camera surveillance	Challenges ability/freedom to develop and follow one's own (moral) judgment
Disproportional power of employers over employees due to use of automated camera surveillance	Challenges ability to follow one's own judgment and to develop a sense of identity in relation to one's work
The exercise of power by members of a household over other members of that household, or by neighbors over other neighbors, using automated camera surveillance	Challenges ability to develop and follow one's own judgment. Violates informational control and therefore challenges ability to own life story
Personalized marketing using CV	Challenges ability to develop and follow own judgment

contact emergency help; or smart doorbells that show you who is in front of your door. These technologies bring surveillance into the private sphere and offer tech companies an insight into people's private lives. Moreover, these video analytics applications change the power dynamics present in social relations. In some cases, this can be empowering. For example, smart home security with fall detection makes elderly people less dependent on caretakers, which can be professionals, but also their family or neighbors. However, smart camera surveillance in the private sphere can also change the power dynamics in social relations in ways that can hurt people's autonomy. For instance: smart camera surveillance gives parents more power over their children, because it enables them to watch their kids even when they are not at home. This gives children less anonymity and less freedom to act as they wish to, both of which children need to develop a sense of identity and autonomy. Another example: smart doorbells not only tell someone who is ringing their doorbell, they often also film the entire lawn or a part of the street and sidewalk. By doing so, smart doorbells provide data of the mail carrier's face or about the neighbor's visitors. Such peer-to-peer surveillance (also known as 'horizontal surveillance') not only violates people's privacy and informational control, it also creates an asymmetrical relation of knowledge and power between neighbors.

In addition to its use for surveillance, CV can also serve business and marketing tools like personalization, that enable companies to influence or manipulate consumer behavior. An example of this is the use of facial recognition to identify and categorize customers, on the basis of which those customers can be targeted with tailored advertisements or deals. Depending on how strong or successful the influence of such targeted or personalized products and services is, we can call this an exercise of power as well. It is problematic when companies have too much power over consumer behavior, because it takes away consumers' ability to make their own, autonomous decisions. See Table 2 for an overview of CV's potential normative implications related to episodic power.

6 Systemic power

In this section, I discuss how CV creates or contributes to systemic power and when this stands in the way of emancipatory progress. The systemic view of power focuses not on individual exercises or instances of power, but on the structural power relations that are reflected in the norms, practices, and institutions that rule a society. Systemic power affects autonomy by determining what opportunities people have, the values people adopt and shape themselves after, and the kinds of choices people make. For instance: the dominance of traditional gender norms in relationships and societal institutions can keep women from pursuing a career. So systemic power is relevant in the context of emancipation, mainly because it plays a crucial role in people's ability to shape their own lives and identities. Just like other aspects of power, systemic power is not necessarily morally problematic. Societal systems are always going to shape people's lives in some way, but emancipation requires that opportunities are available to develop oneself and flourish. Emancipatory progress also requires that people are able to go against certain ways of life, that is, to contest systemic power.

For starters, CV can strengthen the systemic power of institutions such as governments and businesses. CV applications like automated surveillance cameras or bodycams can support governments' systemic power by making law enforcement more efficient and effective. CV can support business intelligence tools or personalized services, which can help businesses to increase profit and improve their market power. Moreover, the companies that develop CV applications increase their market power by selling their products to smaller industries and governments and by acquiring immense amounts of valuable data on people's appearance, expressions, and whereabouts.

When a government, company, or a whole industry has significant systemic power, they are able to determine societal norms and practices. Over the past decades, big tech companies became so powerful that they were collectively able to give rise to a new mode of capitalism: surveillance

capitalism [26]. The surveillance capitalist business model consists of the datafication and commodification of people's behavior as they interact with digital technology. So far, surveillance capitalists mainly datafied and commodified people's online behaviors (such as search queries and online shopping behavior). However, CV can contribute to the rise of surveillance capitalist practices outside of the online sphere, by datafying people's appearance: from the way they walk to the way they dress, and from facial recognition to emotion recognition. The market power of big tech companies makes it difficult to compete with their businesses and makes it challenging for individuals to escape or contest surveillance capitalism. Furthermore, surveillance capitalists have used their systemic power to reify their practices, by leading people to believe that there is no alternative. Despite concerns about privacy and data-ownership, surveillance capitalist practices have been more or less accepted by societies. One could say (as Zuboff does) that this acceptance stems from the fact that people are led to believe that there is no alternative to surveillance capitalism. People were made to believe that, if they want to enjoy (free) digital services, they need to accept the datafication and commodification of their behaviors and characteristics. This reification also prevents the masses from questioning, criticizing, or countering the status quo. This systemic power of big tech companies and surveillance capitalism can stand in the way of people's self-legislation.

Another reified systemic power relation between user and developer is the fact that tech companies usually exercise full authority over the development of the technologies that come to dominate nearly everyone's lives and societies. It does not have to be this way. Alternatively, individuals or policy makers are given a much stronger say in which technologies are developed and the details of their design [16]. The systemic power of big tech companies to determine which (CV) technologies come to dominate people's lives and societal practices, stands in the way of citizens' collective self-legislation.

Furthermore, CV applications sometimes reflect and even exacerbate pre-existing systemic societal injustices. A vivid example of this is the problem of algorithmic bias. Particularly infamous examples of algorithmic bias are biased facial recognition systems, that have often shown to be more likely to recognize White people and males than darker skinned persons and females (e.g. [3]). These biases have led to false arrests by law enforcements agencies in the US that used facial recognition to detect criminal offenders, but also to countless demeaning cases where Black people were categorized as 'gorillas' or 'apes' or Asian people as constantly 'blinking'. The categories used by facial recognition systems also often confirm problematic social stereotypes. For example, darker skinned people are more likely to be given a label associated with crime or violence. Also, many gender categorization systems are binary, which is obviously a problem when the subject in question identifies as non-binary. By maintaining or exacerbating systemic injustices, CV systems can harm people's self-development. Self-development is compromised either because algorithmic biases keep people from exercising certain freedoms or getting equal opportunities (e.g. when biased systems are involved in hiring practices), or because they harm a person's sense of self-worth (e.g. when falsely recognized as criminal by law enforcement or when given demeaning labels by personal devices).

CV applications also reinforce existing societal power structures to the extent that they normalize certain behaviors, views, or identities. Based on visual data, among others, AI systems can stimulate particular behaviors and recommend specific courses of action. For example, semi-automated vehicles can recommend certain actions based on what is happening on the road, which in turn can normalize rather safe or rather dangerous driving styles. Similarly, augmented reality applications could normalize specific behaviors by suggesting courses of action in response to the real-world environment (e.g. "there's your neighbor, say hi!"). Furthermore, CV systems categorize people in accordance with demographic information such as gender, age, race or religion, but also according to other characteristics that one's appearance might reveal, like 'shy', 'poor', 'fashionable', and so on. These labels could reflect and confirm societal stereotypes and norms. Take the aforementioned example of binary gender categorization systems, these reflect and reinforce the norm that a person is either male or female (and, arguably, that it is important to categorize people by gender). Normalization by CV applications can hinder people from developing and following their own judgment, as well as hindering the development of an own sense of identity.

Another issue of systemic power is CV's impact on the labor market. First of all, CV, like other technologies, could automate tasks that make certain jobs and professional skills superfluous. Think about the human operators that used to be needed to monitor CCTV footage. While history shows that jobs that are automated are always replaced by new kinds of jobs, automation might still be a serious threat to individuals whose skills become irrelevant on the labor market and who struggle to find other ways to make a living. Secondly, CV has developed immensely in the last decade or so due to the availability of ImageNet—a large database with labeled images that can be used to train CV models on. ImageNet, in turn, is made possible by the use of crowd sourced workers who label images in return for a small compensation. In both cases it is the scale of the data needed to develop CV and the scale with which CV is and will be implemented, that makes CV able to impact jobs or labor at a systemic, market level.

Finally, the environmental cost of data storage and processing is an important matter of systemic power as well. As Crawford writes: "The massive ecosystem of AI relies

Table 3 Systemic power

How does CV tie into systemic relations or structures of power in society?	How do these systems of power impact people's autonomy?
CV could extend the reach of surveillance capitalist practices and thus increase the systemic power of surveillance capitalists	Limiting people's ability to escape surveillance capitalist practices or to counter or criticize their role in everyday life and society
Tech companies determine which CV applications come to dominate people's lives and societies	Limiting collective self-legislation of citizens
Biased CV algorithms	Limiting self-development because of a lack of equal opportunities or harms to self-worth
CV normalizes certain behaviors and identities	Limiting formation of own judgment and own identity
CV is part of a system of power that has significant environmental costs	Violates human self-legislation to the extent that activist individuals or groups do not stand a chance when trying to counter the environmental impact of AI and big data
CV can cause lasting changes in specific job markets	Limits the self-development and self-legislation of those forced to re-educate themselves, change industries, or work for an exploitative wage

on many kinds of extraction: from harvesting the data made from our daily activities and expressions, to depleting natural resources, and to exploiting labor around the globe so that this vast planetary network can be built and maintained." [6, p. 32]. CV, like other forms of data analytics, relies on big data. Therefore, CV contributes to the environmental damage done by the processing and storage of big data. This is an issue of systemic power: the growing societal dependence on AI maintains a system of power between humans and the environment, that cannot be fought by those trying to protect the environment. The central harm here is obviously environmental harm, but the systemic power of the AI industry simultaneously violates human autonomy, because activist individuals or groups do not stand a chance when trying to counter the environmental impact of AI and big data. See Table 3 for an overview of the issues discussed in this section.

7 Constitutive power

Constitutive power is a view of power that is often associated with the work of Foucault. Constitutive power concentrates not on having or exercising power, but on the effects of power on those subjected to it. Moreover, it looks not at the oppressive side of power (on the fact that A's power keeps B from doing x), but on the creative side of power (namely the fact that A's power makes B do y instead of x). Because of this focus, the constitutive view of power complements the aforementioned aspects of power. Looking at the constitutive aspect of power is ethically relevant, because the ways in which we are moved to act, think, or shape our identity can be normatively laden. Being aware of this normativity enables one to criticize it.

A first way in which computer vision constitutes our behavior, thoughts or identity is through surveillance.

I already touched upon this issue above. Surveillance cameras usually represent a certain authority—the state, the security staff of a shopping mall, an employer, one's parents, and so on. Upon seeing a surveillance camera, a person might alter their behavior out of respect for the authority or because of the threat of repercussions (e.g., getting a fine or getting fired). But surveillance cameras not only cause people to alter their behavior in particular instances, they can also lead to the long-term internalization of official rules or social norms of conduct. Hence, computer vision enforces certain behavioral norms (as also pointed out in the previous section). Although the enforcement of behavioral norms can help to establish a safer environment, it can also support undesirable or unreasonable norms about being a good citizen, employee, child, etc., that are too restrictive with regards to people's ability to form and follow their own judgment and constitute their own identity.

Second, computer vision is not yet a much used technique in the context of personalization. However, it has the potential to provide effective input for personalization, by analyzing a person's appearance (from clothing style to facial expression) and behaviors (from the way a person walks to the things they focus their eyes on). Computer vision namely makes it possible to make numerous inferences about a person's identity, behavior, and other characteristics, on the basis of which that person can be offered personalized offers, messages, goods, or services. Potentially, it would be able to reveal information about a person that they are not even aware of themselves. Like surveillance, personalization is aimed at nudging or manipulating people's behavior. For instance, personalization could move consumers to buy things they otherwise would not buy or encourage voters to alter their political views. Personalization is inherently normative, because it always promotes a certain product, article, political party, course of action, and so on, as being the best

Table 4 Constitutive power

How can CV applications constitute people's behavior, thoughts, and identity?	How do these constitutive effects impact people's autonomy?
CV surveillance causing the internalization of specific norms	Limiting formation of own judgment and own identity
CV can support personalization	Limiting ability to follow and form own judgment (self-legislation)
Labels assigned by CV can constitute a person's sense of identity	Potentially harmful to self-development
Discomfort of being watched or analyzed can cause behavioral changes	Potentially harmful to ability to act freely

choice for a person. In doing so, it not only shapes specific choices people make (e.g. which shoes to buy or which song to listen to), it can shape their preferences and views in the long term. Recommendation systems can shape our political views, our preferences, and even our beliefs about the world and about truth, which is harmful to people's self-legislation.

Thirdly, some computer vision applications, in particular facial recognition and analysis systems, are aimed at identifying and categorizing people on the basis of their appearance. Such applications can be used in numerous ways: for example to detect suspicious people in an airport, to identify the type of clientele in a store, to personalize products online, or to create fun face filters on social media. The labels a person is given by such tools shape how they are perceived by the world around them, but also shape how they grow to understand and develop themselves. Computer vision can therefore also have constitutive effects on a person's identity and self-development.

Finally, the presence of a camera, whether it serves surveillance or other purposes, creates a sense of constantly being watched. Computer vision could exacerbate this feeling, as automated analysis is more rigorous than a human eye. To some, the sense of being watched is so uncomfortable that it leads them to alter their behavior. This issue is sometimes referred to as 'chilling effects'. However, while 'chilling effects' implies that we refrain from acting at all (e.g. refrain from exercising rights, such as participating in a protest), the discomfort of being watched can also mean we simply behave differently. So computer vision applications can make us change our behavior in ways that were initially not intended by those who developed or implemented the technology. This means that, even when a camera was not meant to make us change our behavior, it still has constitutive power over our behavior. The bigger the discomfort people experience when 'watched' by smart cameras, the bigger the impact on people's ability to act freely. See the summary of potential issues related to constitutive power in Table 4.

8 Conclusion

The aim of this article was to provide an overview of the potential normative implications of CV. Given the wide variety of possible CV applications, the focus of the analysis was predominantly on those CV applications that involve the analysis of persons. To create this overview I applied a critical framework, centered around a pluralistic understanding of power. I identified power dynamics related to CV applications and argued how those power dynamics could impact people's autonomy. Considering how CV might harm autonomy is important to ensure that the technological progress, at least in the field of CV, goes hand in hand with social, emancipatory progress.

A limitation of this approach is that it does not necessarily offer guidance in determining how severe an application's impact on autonomy will really be. Rather, the framework points out *potential* impacts on autonomy, that should each be studied in more detail in practice, to determine the severity of the issue and the possible routes of countering the impact on autonomy and, thus, improving the technology. However, despite this limitation, I conclude that the overview forms a valuable contribution to the literature on AI ethics and on computer vision.

Declarations

Conflict of interest The author declares that there are no conflicts of interest.

References

1. Blank, E.L., Weltz, E., Arias, C.: Computer Vision machine learning and future-oriented ethics. *Honors Projects.* 107 (2019). https://digitalcommons.spu.edu/honorsprojects/107

2. Brey, P.: Ethical aspects of facial recognition systems in public places. J. Inf. Commun. Ethics Soc. **2**(2), 97–109 (2004). https://doi.org/10.1108/14779960480000246

3. Buolamwini, J., Gebru, T.: Gender shades: intersectional accuracy disparities in commercial gender classification. Conference on Fairness, Accountability, and Transparency, pp. 77–91 (2018)

4. Coeckelbergh, M.: AI ethics. MIT Press (2020)

5. Coupland, S., Wakunuma, K., Stahl, B.: Identifying ethical issues during the development of a computer vision based AmI system: A case study. Roots for the Future of Ambient Intelligence - Adjunct Proceedings, 3rd European Conference on Ambient Intelligence, AmI 2009, May 2014, pp. 290–297 (2009)

6. Crawford, K.: Atlas of AI: power, politics, and the planetary costs of artificial intelligence. Yale University Press (2021)

7. Crawford, K., Paglen, T.: Excavating AI: The politics of Images in Machine Learning Training Sets. excavating.ai. (2019). Accessed 31 Oct 2022.

8. Doyle, T., Veranas, J.: Public anonimity and the connected world. Ethics Inf Technol. **16**, 207–218 (2014). https://doi.org/10.1007/s10676-014-9346-5

9. Dubber, M.D., Pasquale, F., Das, S. (eds.): The Oxford Handbook of Ethics of AI. Oxford University Press (2020). https://doi.org/10.1093/oxfordhb/9780190067397.001.0001

10. Dufresne-Camaro, C., Chevalier, F., Ishtiaque Ahmed, S.: Computer Vision Applications and their Ethical Risks in the Global South. Graphic Interface Conference. (2020). https://openreview.net/pdf?id=QLFSDNIvI

11. Gordon, J. S., Nyholm, S.: Ethics of Artificial Intelligence. Internet Encyclopedia of Philosophy. (2021). https://iep.utm.edu/ethic-ai/

12. Hale, B.: Identity crisis: face recognition technology and freedom of the will. Ethics Place Environ. **8**(2), 141–158 (2005)

13. Haugaard, M.: Power: a "family resemblance concept." Eur. J. Cult. Stud. **13**(4), 419–438 (2010)

14. Huffer, D., Wood, C., Graham, S.: What the Machine Saw: some questions on the ethics of computer vision and machine learning to investigate human remains trafficking. Internet Archaeol. (2019). https://doi.org/10.11141/ia.52.5

15. Lauronen, M.: Ethical issues in topical computer vision applications. Information Systems, Master's Thesis. Jyväskylä: University of Jyväskylä. (2017). https://jyx.jyu.fi/bitstream/handle/123456789/55806/URN%3aNBN%3afi%3ajyu-201711084167.pdf?sequence=1&isAllowed=y

16. Maas, J.: Machine learning and power relations. AI & Soc. (2022). https://doi.org/10.1007/s00146-022-01400-7

17. Mitchell, M.: Artificial Intelligence: a guide for thinking humans. Pelican Books, London (2019)

18. Moraes, T.G., Almeida, E.C., de Pereira, J.R.L.: Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. AI Ethics (2020). https://doi.org/10.1007/s43681-020-00014-3

19. Morriss, P.: Power: a philosophical analysis. Manchester University Press, Manchester, New York (2002)

20. Müller, V.: Ethics of Artificial Intelligence and Robotics. In: Zalta, E. N. (ed.). The Stanford Encyclopedia of Philosophy. 1st edn (2020). https://plato.stanford.edu/entries/ethics-ai/

21. Sattarov, F.: Power and technology: a philosophical and ethical analysis. Rowman and Littlefield International, London, New York (2019)

22. Selinger, E., Leong, B.: The ethics of facial recognition technology. In: Véliz C (ed) The Oxford Handbook of Digital Ethics (forthcoming). https://doi.org/10.1093/oxfordhb/9780198857815.013.32

23. Skirpan, M., Yeh, T.: Designing a moral compass for the future of computer vision using speculative analysis. In: IEEE Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), pp. 1368–1377. (2017). https://doi.org/10.1109/CVPRW.2017.179

24. Stanley, J.: The Dawn of Robot Surveillance. AI, Video Analytics, and Privacy. American Civil Liberties Union. (2019). https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf

25. Waelen, R.: Why AI ethics is a critical theory. Philos. Tech. (2022). https://doi.org/10.1007/s13347-022-00507-5

26. Zuboff, S.: The age of surveillance capitalism: the fight for a human future at the new frontier of power. Profile Books, London (2019)