The Uncanny Return of Physiognomy

Oliver Bendel
School of Business FHNW, Bahnhofstrasse 6, CH-5210 Windisch
oliver.bendel@fhnw.ch

Abstract

Face recognition is the automated recognition of a face or the automated identification, measuring and description of features of a face. In the 21st century, it is increasingly attempted, whether consciously or unconsciously, to connect to the pseudoscience of physiognomy, which has its origins in ancient times. From the appearance of persons, a conclusion is drawn to their inner self, and attempts are made to identify character traits, personality traits and temperament, or political and sexual orientation. Also biometrics plays a role here. It was founded in the eighteenth century, when physiognomy under the lead of Johann Caspar Lavater had its dubious climax. In this article, the basic principles of this topic are elaborated; selected projects from research and practice are presented and, from an ethical perspective, the possibilities of face recognition are subjected to fundamental critique in this context, including the above examples.

Introduction

Face recognition (or facial recognition) as the automated recognition of a face or as the automated recognition, measuring and description of features of a face has a certain tradition, and its beginnings range back to the 1990s (Bendel 2017a). Recently, this tradition has been extended to ancient times, because ideas are taken up, which have already been disseminated in pseudo-Aristotelian and Aristotelian texts.

The culmination of these ideas, comprising physiognomy and biometrics, happened in the eighteenth century, and they had their nadir in the time of National Socialism. Faces and heads are to be interpreted and measured to determine the character or the sexual or political orientation, i.e., systematic connections between the exterior (in the sense of her or his visible characteristics) and the interior (in the sense of his or her spiritual condition) of a person. Artificial intelligence (AI) is used to revive this pseudoscience.

What is worrying in this context is that the researchers in this field seem to have a certain success. However, if you look more closely, you notice that not only faces and heads are interpreted, but mostly additional attributes (referring to clothes and hairstyle) and data (e.g., from statistics) are gathered, which also forward and solidify prejudices (Brien 2016).

From the point of view of ethics, face recognition must be subjected to a fundamental critique in this context, because the associated methods and implications are able to sustainably unsettle and change society and its members. Arguments, as they are presented here, should be incorporated into social and political opinion formation.

Basics of Facial Recognition

Face recognition is the automated recognition of a face in the environment or in an image (which is already present or produced for the purpose of facial recognition). It is furthermore the automated identification, measurement and description of the features of a face in order to recognize a person ("face recognition" in the strict sense) or his or her gender, health, origin, age, sexual orientation or emotional situation ("emotion recognition", often in connection with facial expression recognition) (Li and Jain 2011; Bendel 2017a).

It is controversial, however, whether one can find something with high security or only with some probability. Undeniably, face recognition is extremely potent in combination with further analytical approaches and data sources (clothing, environment, digital identity, etc.).

Facial recognition uses systems (including facial recognition software and hardware such as cameras and laser or ultrasonic sensors) with two- or three-dimensional detection and measurement techniques (Li and Jain 2011; Bendel 2017a). Eyes, nose, mouth, ears, chin, forehead, hairline and cheekbones are identified and measured and their position, their distance from each other and their respective position to each other are determined. It is also possible to consider the shape of the head and the texture or color of skin, hair and eyes. Overall, more and more complex calculations and approaches of machine learning (neural networks and deep learning) are used.

Face recognition is used for technical devices and for accesses and controls of all kinds for identification and authentication, i.e., in the context and for the purpose of security (Feng and Prabhakaran 2016). It is checked whether the face of a concrete person is present in the picture or in the environment and whether this person has an authorization or whether there is a warrant for arrest for him or her under scrutiny (Bendel 2017a). Also for the sorting of photographs and objects in the broadest sense, facial recognition software is suitable. It depends on the particular application whether the recognition of a face suffices or whether the recognition of a face of a particular sex, age, etc. or a specific person is asked for. In the economy, face recognition is relevant, for example, in interactive advertising spaces, with the aim of personalized advertising and individual advice (Marlow and Wiese 2017; Bendel 2017b).

Facial recognition software is useful to establish orders and allocations, in the regulatory, operational and private context. From a political, legal and ethical point of view, the identification of individuals in the private and public space is controversially discussed (Bendel 2017a). A smartphone and a smart cam that recognize a face can forward data of the face and the person as well as metadata. This allows to check, track and monitor suspects and non-suspects. In addition, the aforementioned facial and head characteristics as well as the behavioral patterns can be analyzed. A detailed discussion from an ethical point of view takes place in the penultimate section.

Basics of Physiognomy

Physiognomy is a pseudoscience that wants to draw conclusions on the character and personality traits as well as the temperament of a person from his or her appearance, especially from the form of the head and the peculiarities of the face (Belting 2013; Schmölders 2007; Campe and Schneider 1996; Schwertfeger 2006). Everyday observations and experiences, which are partly biased and doubtful, are systematized and generalized.

Already in ancient times, physiognomy found strong proponents, as well as in the Middle Ages and the Renaissance in the context of humoral pathology (the theory of the four humors), which is based among other things on Galenus (second century after our time); in the age of the Enlightenment, physiognomy flourished with Johann Caspar Lavater as its main representative. The pastor from Zurich became famous and notorious with his four volumes on "Physiognomic Fragments". He is the originator of the nonsensical and powerful assertion that beauty and morality are correlated, a beautiful human is also good, an ugly human is evil, and thereby bringing together and jumbling the objects of ethics and aesthetics (Schmölders 2007).

Also in the eighteenth century, Peter Camper from the Netherlands came to be known. He founded biometrics, with biometry as its object, the measurement of the biological or naturally given (Belting 2013). In his speech at the Amsterdam Academy of Arts, about the natural difference between the facial features of people of different ages and different regions, he described his alleged discovery that the different human races can be distinguished with the help of quantifiable shape characteristics of the skull. Among other things, the Dutchman was interested in the intelligence of people and groups and, from today's point of view, presented discriminatory and racist considerations.

Finally, in the nineteenth and twentieth century, physiognomy, biometrics and genetics were most definitively used as a supposedly scientific base for racism and eugenics (Belting 2013; Schmölders 2007; Campe and Schneider 1996). In the second half of the nineteenth century, the Italian doctor Cesare Lombroso believed – because of his research and interpretations of faces – to be able to recognize whether someone was a criminal or not. Subsequently, he became particularly powerful, and to this day, certain circles prefer to expose a criminal before he or she can turn into a criminal, which is not the only paradox in this context.

Under the keyword "Menschenkenntnis" ("knowledge of human nature"), physiognomy gained renewed popularity in the 1920s and 1930s (Belting 2013; Schmölders 2007; Campe and Schneider 1996). Together with works on graphology, compilations of old and new writings about physiognomy became bestsellers, and in many areas and contexts, physiognomy was no longer a harmless social game, but resulted in the systematic disqualification and rejection of pupils and applicants. As a teenager in Germany in the 1980s, the author was told by his female teacher that his handwriting, which pointed to the left, was evidence of a bad character. From then on his writing pointed to the right, which in turn proves the questionability of such statements, because he did not change his character. Examples from the present are the psycho-physiognomy founded by Carl Huter, and the so-called pathological physiognomy.

Physiognomy can be distinguished from pathognomy, which was represented by the German poet and scholar Johann Wolfgang von Goethe. Lavater and Goethe were in exchange, and the German had visited the Swiss in Zurich and encouraged him in his ideas, but then later turned against them. Pathognomy does stem from the immutable properties of the bone and cartilage structure, but from the traces supposedly left on the body and face by feelings, the center of one's life, lifestyles and professional and social status. Physiognomy can also be distinguished from the facial expression as a doctrine that deals with the expression spontaneously formed by the facial muscles, precisely the facial expression per se.

Current Projects in Research and Practice

Here are three projects that have caused a stir in recent years. They were, therefore, chosen according to the attention that they aroused, whereby an economic or scientific activity was a prerogative. In addition, special attention was paid to the fact that different aspects are sometimes relevant. It makes sense to investigate further projects in other contributions and to evaluate them from an ethical perspective.

Faception

The company Faception, based in Tel Aviv, has developed a biometrically working and self-learning facial recognition software that supposedly can read from the face, whether someone is gentle or aggressive (Meyer 2016). Among other things, the software measures the distances of different points (the descriptors) in the face. It then calculates certain results that are classified as personality traits. This creates an individual "personality score card".

According to the company, the software would have ranked three of the assassins of the Paris attacks in November 2015 with an 80 percent accuracy as terrorists (Meyer 2016). In the Wall Street Journal, the CEO Shai Gilboa said that the human personality was determined by our DNA and reflected in our face (Meyer 2016). This is linked to physiognomy and, via the inclusion of biometrics and genetics, to postulates that were popular in the early twentieth century, and also in times of National Socialism.

The company itself writes on its website (accessible via www.faception.com): "Utilizing advanced machine learning techniques we developed and continue to evolve an array of classifiers. These classifiers represent a certain persona, with a unique personality type, a collection of personality traits or behaviors. Our algorithms can score an individual according to their fit to these classifiers." These "classifiers" are: high IQ, academic researcher, professional poker player, terrorist. They recall the persona from computer science, specifically the human-computer interaction (HCI), a prototype for a group of users, with certain characteristics and a certain behavior.

Jiao Tong University

Xiaolin Wu and Xi Zhang, researchers of the Jiao Tong University in Shanghai, 2016 allegedly taught a software to detect criminals by means of photographs (Wu and Zhang 2016; Brien 2016). In total, 1,856 images of male Chinese aged between 18 and 55 years without a beard were used. Half of these men were criminals. Ninety percent of the images were used to train the neural network, and the remaining ten percent were then utilized for testing.

According to the researchers, the self-learning software eventually could distinguish criminals from non-criminals with an accuracy of 89.5 percent (Wu and Zhang 2016; Brien 2016). This would prove that an automated inference on possible delinquency based on the characteristics of the face is possible, notwithstanding the historical controversy that the two researchers explicitly mention in their paper.

According to the scientists, there are three different facial traits and features that indicate that someone is a criminal: The curvature of the upper lip is expected to be 23 percent greater for criminals than for non-criminals. Moreover, the distance between the two inner corners of the eyes is six percent shorter and the angle between the two lines from the tip of the nose to the corners of the mouth 20 percent smaller (Wu and Zhang 2016; Brien 2016). In this way, concrete parameters for biometric analyses are formulated, so that theoretically fundamental statements about persons would be possible, i.e., not just as a subsequent sorting, but as a current and future allocation.

Due to the enormous media attention, the researchers decided to make further statements and justify their methods and results. Among other things, they said: "Our work is only intended for pure academic discussions; how it has become a media consumption is a total surprise to us." (Wu and Zhang 2017) They regretted the use of the term physiognomy: They "were not sensitive enough to the inherent dirty connotation of the word in the English speaking academia" (Wu and Zhang 2017). However, they had already mentioned in their original paper that this was a pseudoscience.

Stanford University

In 2017, Michal Kosinski and Yilun Wang of Stanford University apparently managed to train a facial recognition software in such a way that it was able to deduce from photos whether the person portrayed is gay or heterosexual (Taschwer 2017; Kosinski and Wang 2017).

For their study, the authors downloaded more than 300,000 portrait photos of up to 75,000 people from an American dating platform. With 35,326 photos of 14,776 people, they fed a VGG-Face, a self-learning software that looks for characteristic "facial fingerprints" and establishes correlations between these "facial fingerprints" and the sexual orientation of their owners (Taschwer 2017). According to the researchers, homosexual males have slightly more feminine facial features, narrower jaws, longer noses and a higher forehead, homosexual women tend to more masculine facial features (Kosinski and Wang 2017). Thus, they as well formulate parameters for biometric analyses.

The researchers write in their summary: "Given a single facial image, a classifier could correctly distinguish between gay and heterosexual men in 81% of cases, and in 74% of cases for women. Human judges achieved a much lower accuracy: 61% for men and 54% for women. The accuracy of the algorithm increased to 91% and 83%, respectively, given five facial images per person." (Kosinski and Wang 2017)

However, if the program had to identify from 1,000 randomly selected men (based on more than five photos per man) those 100 men who were most likely gay, it was often wrong: of the 100 selected men only 47 were actually gay (Taschwer 2017).

As the researchers write in an accompanying text, they pondered a long time whether they should publish their study at all for the following reasons (Taschwer 2017): On the one hand, homosexual people are still discriminated almost everywhere in the world, in some countries they even live in mortal danger. The findings of the researchers "expose a threat to the privacy and safety of gay men and women" (Kosinski and Wang 2017). On the other hand, the ability of a software to categorize people based on their photos constitutes a serious intrusion into the privacy of humans.

Motivations for the Application

The fight against terrorism and the prevention of crimes are obvious motives to revive the approaches of physiognomy and biometrics, as long as they are restricted to facial features and characteristics as well as the shape of the head. The hope is to track down and arrest actual and potential offenders. The dream of being able to fight the bad or the irregular in this way seems to come true. (Kosinski and Wang 2017) point out "that companies and governments are increasingly using computer vision algorithms to detect people's intimate traits".

The truth is, however, that the majority of companies are mainly interested in placing suitable advertisement, e.g., on interactive advertising spaces (Bendel 2017b). They analyze gender, age, origin, emotional state and now other aspects such as sexual orientation as well. There should be clear limits, however, when one imagines that a certain sexual orientation or preference – beyond homosexuality and heterosexuality – could be identified and a corresponding advertisement, such as for handcuffs, could be shown.

In the case of personnel selection and assessment, companies also hope for insights concerning the suitability of applicants and employees. Schneemann (2002) claims that the psycho-physiognomist will recognize the form of a personality trait, for example, in an "outward formation of the skull". In the operational environment, intelligence, creativity, adaptability and subordination play a role. Companies and organizations could be more and more interested in figuring out these traits through face recognition, just as they had previously relied on dubious findings from graphology.

The choice of a partner is another possible motivation to use face recognition. Here not only the reliability and honesty of the future or current partner play a role, but also his or her sexual performance and sexual orientation. In one's search for a partner, one may want to make sure that he or she is actively striving to produce offspring and does not have an outing after a few years, and if one already has a partner, one may want to check if she or he deserves one's trust. Or he or she simply wants to make sure that the chosen partner is also judged by others as attractive (Thomas 2016).

Of course, the relevant software can also be used for entertainment, which is linked to the social games of earlier times, in which you – in the tradition of Lavater himself – drew and implied facial features. Finally it can be enlightening (in individual cases even disturbing) for a person to be categorized and compared by a software. You will learn which possible effect you have on your fellow human beings, and how others perceive you, at least subliminally and subconsciously. This is particularly interesting when it is a matter of gender.

These motives are on very different levels. However, acceptance by the applying individuals as well as by the applying organizations is likely to be relatively high, if appropriate successes had been achieved or simply claimed. States could even come up with the idea of setting such methods as a standard when crossing the borders of a country or in public places and streets.

In Germany, a face recognition project, carried out at the Südkreuz station in Berlin in 2017 with volunteers involving the identification of persons, lead to a controversy. Because of the experience of National Socialism, people are particularly sensitive in Germany regarding the collection and evaluation of data, so that we can assume that approaches of physiognomy would provide a huge outcry. At many airports, for example in Zurich (Switzerland) and in the USA, facial recognition is already in use, although currently it is hardly linked with character traits.

The Ethical Perspective

In the following, the author assumes the perspective of ethics, especially information and technology ethics. After a short explanation of these specific ethics, several problem areas are explored using their central terms.

Information and Technology Ethics

Applied ethics refers to definable thematic areas and forms the specific ethics. Information ethics is about the information society's morality (Bendel 2016). It deals with how we behave or should behave in a moral sense when offering and using information and communication technologies (ICT), information systems and digital media. Key concepts include informational autonomy, digital identity, digital divide and informational self-defense (Kuhlen 2014; Bendel 2016).

Technology ethics refers to moral questions of technology use. It can equally deal with the technology of vehicles or weapons and with nanotechnology or nuclear energy. In the information society, where more and more technologies include computer technologies, technology ethics is closely linked to information ethics or is partially dissipated in it (Bendel 2016).

The concept of algorithm ethics is used partially synonymously with that of machine ethics – a design discipline close to robotics and AI which is not further discussed here (Anderson and Anderson 2011) –, in some cases rather in the discussion about search engines, proposal lists, and big data. Its object, if not considered a design discipline but a reflection discipline, can be largely covered by information ethics.

Further specific ethics, which may be of marginal relevance, are business ethics, science ethics, medical ethics and legal ethics. These are mentioned in the following, without further explaining them and without applying their specific terms and methods.

Use of Personal Data

It is a fundamental question whether it is allowed to simply record a face and analyze it by means of information technology. The personal data, one could argue, belong to the person and may only be collected and processed under specific and controlled conditions. (Kosinski and Wang 2017) have also made aware of the invasion of privacy by this software.

Of course, in every human contact certain data are collected, and stored in the brain for a short or long time and information is transmitted, but in machine processing there are other aspects and possibilities. Thus, potentially many people can access the stored data and the completed analyses, there may be unknown persons involved, the information can be linked and passed on, and the inferences that the systems draw can be wrong or interpreted incorrectly by the responsible authorities. The researchers from Stanford University have explicitly rendered the categorization problematic.

On the whole, it can be said that personal data are withdrawn – in a manner of speaking – from the person concerned, and a digital identity is created (in addition to the digital identity he or she is responsible for), which he or she cannot control, and whose informational autonomy is affected which is the subject of information ethics. Data protection is required at the legal level.

Character as a Specific Feature

The specific question is whether character traits, personality traits and temperament can be determined mechanically. On the one hand, it can be argued that they belong, even more than other characteristics, to the person, insofar as they are his or her essence, and are difficult to change. On the other hand, it could be said that external features such as noses or eyes are visible and that, in their entirety, the facial characteristics result in the individual personality, in the aforementioned examples even permanently. However, character traits are not visible and thus difficult to describe and, if they remain so imprecise, they can be attributed to very many people. It is even the case that a character trait or personality trait, which only a few people possess, indicates a disorder.

On the other hand, one can again argue that, in most cases, not only individual traits are collected, but several in their entirety, which allows an accurate picture. That these, in turn, may be assigned to certain types, like in Faception, is due to the manageability and the difficult descriptiveness, especially of aggregated information, and in the field of IT, as the persona show, not at all unusual. Certainly, data on character traits, when clearly assigned, are personal data, and one must again ask for informational autonomy and privacy.

Apparent Potentials

A sensitive point is that software and hardware seem to find other and even more traits than humans. They seem to see what we overlook, namely both the observed and the observing. This can already be critically determined with regard to the recognition of age and gender.

Thus, the author has repeatedly had the opportunity to test appropriate software with his students. They often were obviously not happy when they were thought to be much younger, which may be just the opposite in older persons. The students were generally furious when given the wrong gender. As an uninvolved third party, one tended to agree with the machine findings, which in turn shows that it can contribute to self-awareness.

It is, however, the question whether it is not preferable for people to tell each other, that he or she differs from his or her self-image; at least this information may be given in a social and communicative setting, for example, when regret is expressed or affection shown. On the other hand, the judgement of a machine can also be received in such a way that no friend knows about it, and the described reactions of the students are likely to have been so pronounced precisely because of the part-public situation, the exposure to friends and colleagues.

From the point of view of information ethics (and on the fringes of technology ethics), one has to question in any case how to deal with the fact that the machines seem to produce new insights, which we have not anticipated, and how a detached digital identity affects our everyday real identity (and the digital identity we are responsible for).

Moral Evaluation of Properties

Furthermore, it can be seen that character traits, personality traits and temperament are often morally judged, which is partly the purpose of the systems used. Thus, these systems allow themselves to pass moral judgements about people, a fact that can be criticized, even if they are moral judgements which the systems are taught or which are actually only passed by the operating persons. Above all, however, the persons concerned are sorted into normative categories, along with the corresponding positive and negative evaluations and conclusions.

Moreover, the systems, which is also investigated under the name of algorithm ethics, will corroborate and spread existing prejudices that are taught to them (O'Neil 2016). We encountered a similar phenomenon when AI was used in beauty contests. Light-skinned women with European facial features were generally preferred (Michel 2016). Information ethics (and on the fringe also media ethics, which has not been further deepened here) can also address these problems.

Rights of Individuals and Groups

The use of this type of approaches to identify terrorists or criminals can be morally justified with the protection of society. You could argue that while the rights of the persons analyzed are being impaired (even if they are perpetrators), the benefits for the community are so high that you can live with it. However, people who have done nothing wrong are targeted again and again, and even with face recognition, it is true that all faces are at least partially analyzed before a suspected person can be tracked down. Thus, one raises a kind of general suspicion, one controls and observes everybody and, if possible, sorts out those about whom no further information is available, which reverses the previously prevailing principle.

This is already true in the case of classical facial recognition – but now also people with certain facial features are suspects, which is very likely against reasonableness. Even if there is a statistical relationship between the appearance and the inside of a person, this does not mean that all have to tolerate an informational access. In fact, the informational autonomy of the uninvolved is violated, which brings information ethics back into play.

Suspicion and Detainment of Persons

A further question is what happens with a person whom the software has identified as suspicious. First, it is evident that a damage has occurred by the fact alone that the person was identified as suspicious, her or his personal information is used without their knowledge or without their consent and he or she will be targeted by the police and the secret service. In addition, in any place, there must occur a further observation or access that may be uncomfortable or might even harm someone's reputation or body. There could be even more harm in store for the person concerned if he or she is deprived of his or her freedom. In this case, the machine determination would not only affect the informational, but also the personal autonomy.

If from the physical characteristics conclusions are drawn to the political or sexual orientation and if these orientations are morally or legally incompatible in a country, this may lead to humiliating or destructive treatment. Of course, access to persons who are harming or intend to harm others must be possible, but the question is whether a mass analysis should be used as the basis of a software. Furthermore, there will be probably more access than before to innocent people. Therefore, information ethics, technology ethics and legal ethics must be incorporated into these discussions.

False Promises

Developers and operators sometimes suggest that some insights are discernible from the face alone. In emotion detection, which bases mostly on facial expression, this is certainly largely the case. The facial expressions are in part innate, in part learned, and they belong – like the spoken language – to our means of communication. Since they belong to our visual means of communication, it is obvious that they can also be understood by optical systems connected to AI, although a poker face is difficult to decipher. In the case of characteristics that physically belong to humans, this is different. When face recognition is mentioned, often more data is actually used, such as clothes and hairstyle or surroundings.

There is a high degree of complexity for the person concerned. It is hard for him or her to judge whether he or she could fall into certain categories that may have negative consequences for him or her. Science ethics must address the false promises and vague representations of the researchers, which can lead to considerable insecurity in the population and excessive expectations in politics. Information ethics must address the use of the specific procedures.

Questionable Categories

Furthermore, the categories are questionable in one or the other project. A highly intelligent person can easily be quite dangerous, violent, and criminal. Categories, such as in Faception, which distinguish between highly intelligent individuals and terrorists, suggest that these are different, even contradictory, categories. Furthermore, the persona from the HCI is recurringly criticized as being an unauthorized simplification.

In principle, moral and legal categories are repeatedly mixed and confused. A criminal person is not per se evil or abnormal, but simply someone who violates the law, consciously or unconsciously. A person who becomes a criminal can also be moral in the true sense, especially if he or she decides and acts in an unjust state or unjust system. (Wu and Zhang 2016) write in their original paper that "being a criminal requires a host of abnormal (outlier) personal traits"; in their defense, they emphasize that "a caveat about the possible biases in the input data should be issued" (Wu and Zhang 2017).

The fact that these things are not systematically separated could be based either on economic interests or on political ideologies. For totalitarian states, it is usually evident that violations of the law are also breaches of morality. Here science ethics, with a view to the responsibility of researchers, and legal ethics, with a view to the mingling of law and morality, are required. Information ethics addresses the extent to which information systems and software tools of this type require and promote a questionable categorization, and how one could adapt it, or eliminate it.

False Findings and Dubious Comparisons

The basic question is what to do with the truth that some systems, under whatever conditions and with whatever methods, simply produce false statements and predictions. The fact that they achieve a certain success in 50 to 70 percent of the cases may sound promising to some ears, but cannot conceal the fact that they are mistaken in 50 to 30 percent. This is not just a marginal but a huge gap.

It is also important to bear in mind that these are specialized systems that are mostly compared to people who are not specialized. Many of us simply do not care what sexual orientation someone has, and accordingly, we do not use our energy to recognize the sexual orientation of people who do not qualify as partners. However, if we are trained, as customs officers or passport inspectors, to shift to another area of application, we can see discrepancies and feelings better than the average person can.

Thus, it is advisable to compare specialized systems with specialized individuals. Once again, science ethics (hence economic or business ethics) is required, which examines the falseness of the findings as well as the questionability of the comparisons.

Imbalance between the Parties Involved

Another problem is the imbalance between the observer and the observed, which expresses itself at different levels. The observed does not have the technology that the observer has, he or she does not know in detail the functionality, and he or she does not know to whom the data will be passed on. In many cases, there is only superficial information, such as the indication that a camera is present. In many countries and areas not even that is established, not even there where it is a regulation (Morchner 2010). As a concerned person, one is under-informed and defenseless.

From an ethical and legal perspective, one can demand that the operators inform the public about the existence of the cameras and the analysis by AI, but some might argue that they give up advantages and help suspects to become unsuspicious. For them, the imbalance is, so to speak, program. Here, too, informational autonomy is at risk, and there is a digital gap of a special kind, namely between technology users and technology-used. Here, both technology and information ethics are required. The latter could use the discursive method to disclose the interests of parties and help make evaluations (Kuhlen 2004).

Informational Self-Defense

The informational self-defense arises from the digital disobedience or constitutes an independent action in the heat of the moment, and serves the preservation of the informational autonomy and the (self-constructed) digital identity (Bendel 2016). For example, you could tear off the data glasses of people walking towards you, because they might record you, could stop cars whose cameras have recorded you and ask for data deletion, or you are as a fake on such platforms that use the personal data for economic purposes. Whether mitigating circumstances or even claims for impunity are to be asserted in the event of damage or infringement will be decided in individual cases. A term with an additional meaning is "digital self-defense".

People will take a stand against face recognition systems. They will cover up themselves, if still legally authorized, they will apply makeup, will get tattooed and affix jewelry, will have optical operations performed and use technical means to try to disrupt and influence the systems. If they do not commit themselves to self-defense, then perhaps to the somewhat weaker concept of information thrift.

The Renaissance of Physiognomy

It becomes obvious that the physiognomy of ancient times, the Middle Ages and the Renaissance has resurrected and finds its representatives and propagators. Above all, the questionable excesses of the Enlightenment and the nineteenth and twentieth century have resurfaced, in which face, race, intelligence and worth were combined.

This development seems quite strange today. In Europe, they rub their eyes when seeing the ghosts that they seem to have successfully banished. In the United States, where diversity plays a major role, where discrimination on grounds of origin, age and gender is ostracized and punished, they see themselves in a great dilemma that is also expressed in the caution of the researchers from Stanford University. Here, social-political claims, whether they are exaggerated or not, clash with technical possibilities. At the same time, in some circles in the US, some states and sensitivities that have arisen in Europe in the course of history may meet with a certain lack of understanding. In spite of this, it could be of interest to them – as well as to researchers from other parts of the world – to study the European idea and intellectual history under these considerations.

What obviously drives this development are economic and political interests. In times of the greatest uncertainty, one hopes more than ever to have simple procedures with which – if it is not simply a question of maximizing profits – the supposed evil can be fought against. This is combined with the potency expected from AI, and with the effectiveness and efficiency of machine processes. In addition to the self-assumed possibilities, opportunities play a role that one can claim in front of others: one can persuade the population that it is possible to fight terror with technical means. Information ethics can use the discursive method to disclose the interests of the parties involved and to help assess the adequacy of the means on all sides (Kuhlen 2004).

Summary and Outlook

Face recognition has become a big topic. Now, its direction is changing more and more. To a large extent, the machine-based approaches in their categorizations and functionalities are very questionable. Thus, moral and legal approaches are messed up, in some places it is suggested that criminals are basically bad people, even though they only violate certain laws. Moreover, it is suggested that the machine can read faces better and faster.

In certain questions such as the sexual orientation, a software seems to actually perform this determination better than a human does. However, as it turned out, the person does not necessarily have an interest in this determination. Moreover, it is also helpful or even essential for the software if it receives additional data that have nothing to do with the face and the head. These, in turn, may be of discriminatory character.

In the end, there are many reasons not to use face recognition at all to determine character traits, personality traits and temperament as well as sexual orientation. At the very least, however, there are many ethical questions that were dealt with in this article to some extent, and which may reverberate in political considerations.

References

Anderson, M.; and Anderson, S. L. eds. 2011. *Machine Ethics*. Cambridge: Cambridge University Press.

Belting, H. 2013. *Faces*. Eine Geschichte des Gesichts. München: C. H. Beck.

Bendel, O. 2017a. Gesichtserkennung. *Gabler Wirtschaftslexikon*. Wiesbaden: Springer Gabler. http://wirtschaftslexikon.gabler.de/Definition/gesichtserkennungssoftware.html.

Bendel, O. 2017b. Neue Spione in den Straßen, auf den Plätzen und in den Läden: Interaktive Werbeflächen aus ethischer Sicht. *Telepolis*, August 15, 2017. https://www.heise.de/tp/features/Neue-Spione-in-den-Strassen-auf-den-Plaetzen-und-in-den-Laeden-3797118.html.

Bendel, O. 2016. *300 Keywords Informationsethik: Grundwissen aus Computer-, Netz- und Neue-Medien-Ethik sowie Maschinenethik.* Wiesbaden: Springer Gabler.

Brien, J. 2016. Gefährliches Spiel: Eine KI hat gelernt, Kriminelle anhand von Fotos zu erkennen. *t3n*, November 24, 2016. http://t3n.de/news/ki-kriminelle-fotos-erkennen-769867/.

Campe, R.; and Schneider, M. eds. 1996. *Geschichten der Physiognomik. Text – Bild – Wissen*. Freiburg im Breisgau: Rombach.

Feng, R.; and Prabhakaran, B. 2016. On the "Face of Things". *ICMR'16*, June 06–09, 2016, New York, USA.

Kosinski, M.; and Wang, Y. 2017. Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, 2017. Preprint via https://psyarxiv.com/hv28a/.

Kuhlen, R. 2004. *Informationsethik: Umgang mit Wissen und Informationen in elektronischen Räumen.* UVK/UTB, Konstanz 2004.

Li, S. Z.; and Jain, A. K. eds. 2011. *Handbook of Face Recognition*. London: Springer.

Marlow, J.; and Wiese, J. 2017. Surveying Surveying User Reactions to Recommendations Based on Inferences Made by Face Detection Technology. *RecSys'17*, August 27–31, 2017, Como, Italy. pp. 269 – 273.

Meyer, J.-B. 2017. So, wie Sie aussehen, sind Sie ein Terrorist! *Computerwoche*, June 7, 2017. https://www.computerwoche.de/a/so-wie-sie-aussehen-sind-sie-ein-terrorist,3229425.

Michel, C. 2016. Rassismus? Beim KI-Schönheitswettbewerb gewinnen fast nur Weiße. *Wired*, September 9, 2016. https://www.wired.de/collection/life/rassismus-beim-ki-schoenheitswettbewerb-gewinnen-fast-nur-weisse.

Morchner, T. 2010. Streit um Kennzeichnung von Überwachungskameras in Hannover. *Hannoversche Allgemeine*, November 23, 2010. http://www.haz.de/Hannover/Aus-der-Stadt/Uebersicht/Streit-um-Kennzeichnung-von-Ueberwachungskameras-in-Hannover.

O'Neil, C. 2016. *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. New York: Crown.

Schmölders, C. 2007. *Das Vorurteil im Leibe. Eine Einführung in die Physiognomik.* 3th edition. Berlin: Akademie-Verlag.

Schneemann, D. 2002. *Wer bin ich? Wer bist Du?: Das große Buch der Menschenkenntnis*. Bonn-Oberkassel: Heel Verlag.

Schwertfeger, B. 2006. Verräterische Beule am Kopf. *Spiegel Online*, November 6, 2006. http://www.spiegel.de/lebenundlernen/job/personalauswahl-per-gesichtsanalyse-verraeterische-beule-am-kopf-a-446426.html.

Taschwer, K. 2017. Software liest aus Porträtfotos sexuelle Orientierung ab. *derStandard.at*, September 8, 2017. http://derstandard.at/2000063816118/Software-liest-aus-Portraetfotos-sexuelle-Orientierung-ab.

Thomas, I. C. 2017. Dieses Computerprogramm verrät, wie schön Sie sind. *Welt*, October 7, 2017. https://www.welt.de/wirtschaft/webwelt/article150754121/Dieses-Computerprogramm-verraet-wie-schoen-Sie-sind.html.

Wu, X.; and Zhang, X. 2016. Automated Inference on Criminality Using Face Images. *arXiv*, November 13, 2016. https://arxiv.org/abs/1611.04135v1.

Wu, X.; and Zhang, X. Responses to Critiques on Machine Learning of Criminality Perceptions. *arXiv*, May 26, 2017. https://arxiv.org/abs/1611.04135v3.