LAW

and

ORDER

The »Criminal Law« of predictive society

… or how »smart« algorithms (could) change the administration of criminal justice

By Christoph Burchard

Applying AI to criminal law and justice – a threatening vision of the future or a utopia of security and freedom?

It is the year 2054. An imminent double murder, a crime of passion, is reported to the pre-cop department of Washington D.C. After consulting a face database and other databases, the detective in charge quickly identifies the perpetrator and the crime scene. A pre-cop team rushes over and at the last minute (the weapon was already being raised for action), they are able to prevent the crime from taking place. The perpetrator is then arrested for the future killing of his wife and her lover. This is the opening of Minority Report, a science fiction thriller from 2002. In it, the pre-crime programme – preventing crimes before they happen – has made crime a thing of the past. »That which keeps us safe will also keep us free« – this is how the programme is promoted: as the perfect reconciliation of security and freedom.

The future is now – even in criminal law and justice!

As fantastical as it seemed in the film – this future has already begun. However, whereas in Minority Report, Hollywood still had to depend on individuals with clairvoyant abilities, today »smart« algorithms are employed. Driven by artificial intelligence (AI) and ever faster computational possibilities, they are able to analyse large and apparently unconnected datasets (big data) in such a way that individual behaviour can be predicted with increasing accuracy.

This has long been established in many areas of life: who will buy what online? Who will with what probability be unable to repay their loan? These questions, directed at the future, are answered algorithmically in the present, in order to be able to »re«-act immediately. In these areas, our society is being transformed into something like algorithmic predictive society. Traditionally, uncertainty about how the future will develop is processed by human prognoses, and also by trust in certain institutions, especially the law. In predictive society, this task is assumed by probability calculations from »smart« algorithms, whose capabilities far exceed human data processing capabilities. In predictive society, therefore, the accuracy of the algorithms and the availability of the necessary data are the actual currency, and consequently the actual source of societal power.

Criminal law is no exception here. The »criminal law« of predictive society is already in the making. Here are just a few examples:

- Predictive and big-data policing promises to be able to identify crime scenes (abstract) as well as victims and perpetrators (individually) before the crime is committed. In this manner, patrol cars should be able to be sent to hotspots before break-ins etc. occur. These kinds of programmes are being used globally, including in Hessen, where we use software from the US provider Palantir, making ourselves to some extent dependent on such firms in the process.

- Risk assessment programmes promise a more precise estimate of the harmlessness/dangerousness of criminals. Those posing a threat to society should removed from society longer, harmless criminals released from custody sooner or put on parole from the start. This not only provides security, it also saves money – which is the reason that these programmes are already being widely applied in the USA.

- Government agencies are not alone in relying on predictions to prevent crime; in fact, the government is a shrinking subset of predictive society. Crime prevention and even more importantly pre-emption are both being »privatised«. Monitoring programmes are being developed for grocery stores among other things in order to identify shoplifters before they shoplift. And predictive policing algorithms can also be used by employers. The buzzword is digital criminal compliance: the digitally supported real-time prevention of compliance violations such as corruption in business dealings or market manipulations.

- But the risk emanating from potential perpetrators is not the only future that can be determined predictively. Judges and prosecutors are increasingly viewed as a risk because they may evaluate subjectively and with bias – be swayed, for example, by racial prejudice. There are considerations to review the relative reasonableness of penalties by algorithm before they are imposed. This falls on sympathetic ears in Germany, too. After all, penalties vary significantly throughout Germany, and not just between north and south.

»Thou shalt not kill!« – becomes »Thou cannot kill!«

How should one react to all these developments? A frequent reaction is the with the defence of one's vested interests: »Algorithms can't do what experienced crime officers and experts (judges, prosecutors, defence attorneys, etc.) can do. Algorithms cannot grasp the complexities of penalties, not to mention let common sense prevail.« So one hears, time and again. But this is often just whistling in the dark.

Can crimes really be predicted? In 2002, Tom Cruise plays a police officer in »Minority Report« who himself gets caught in the machinery of the pre-crime programme. The movie takes places in the year 2054 and is based on a short story from 1956.

Algorithms in the administration of criminal justice may be accompanied by considerable shifts in power, especially to the benefit of those actors »behind« the algorithms – such as the IT company, which in the USA does not even have to make the algorithmic foundations of its risk assessment programmes public (!). Democratic lawmakers must also be taken into consideration, however. They would seem to be able to »finally« govern completely through algorithms. Defending vested interests (»We have always done it this way!«) is, however, not an argument against the »criminal law« of predictive society. Even less so, when this appears to fulfil the promises of criminal justice better than the original. Where criminal law can only operate contra-factually and normatively (»Thou shalt not kill! But you can.«), predictive society promises factuality (»Thou cannot kill!«).

Technically, these promises are still difficult to fulfil. In the USA, predictive policing programmes have already been discontinued because they have not proven to be sufficiently effective. Comprehensive face recognition is switched off, because it is discriminating for technical reasons. And it has become clear that risk assessment algorithms are not – as had originally been hoped for by citizen rights movements – a valid means for overcoming the deeply rooted racism in the US criminal justice system. Predictions »today« are normally only as neutral as the data that was collected »yesterday«. If the data input is racist, the prediction output is also racist (bias in, bias out – or more bluntly: crap in, crap out). If this is coupled with blind faith in technology, the bias – such as a racist bias – of the prediction goes socially undetected.

As serious as these objections are, they are ineffective overall against the new »criminal law« of predictive society. They act instead as arguments for technological development and more innovation. The causes and justifications for more prediction in the administration of criminal justice remain unaffected. Certainly, smart algorithms are like a black box, whose prognoses cannot be comprehended – but doesn't the court also make its sentencing decisions in closed chambers? And yes, algorithms may be prone to error and bias – but doesn't this apply even more to judges, who are also »only« human?

Where does the need for algorithms come from?

WWhat drives us, then, to »criminal law« in predictive society? A lot is probably due to the complex relationship between »trust and conflict«. It also has to do with how legal systems or algorithms process and reduce social complexities – future uncertainties, in other words.

The social acceptance of predictive society goes hand in hand with the loss and shifting of trust. Trust in others is lost when they are no long viewed as fellow citizens, politicians (lawmakers) or judges (law appliers), but rather as risks. This brings other actors into play (such as private »code makers« and »code appliers«). In addition, mistrust toward law as a means of reducing social complexity is growing – especially when law becomes politicised and is either unable or unwilling to negotiate social conflicts neutrally. The less social conflicts are able to be confined as legal conflicts and thereby neutralised, the greater the trust in the neutrality of code and IT (»In code and technology we trust!«), even if code and IT are actually thoroughly normative. This applies all the more as algorithmic predictions (so we are constantly promised) are even better and more effective than law at providing security in the future.

The fact that the transition to predictive society means an increase in surveillance trends (no predictions without data!) seems to be acceptable to many. What is decisive in this regard is

IN A NUTSHELL

- We are underway toward becoming an »algorithmic predictive society«: artificial intelligence and big data lead to increasing algortihmic predicitons of future behaviour so that we can »re«-act to them in the present.
- The more trust in the constitutional state diminishes, the more society relies on the purpoted efficiency and objectivity of algorthmic predictions to generate future security.
- Justice and police use prediction algorithms for the purpose of predicting crime and the dangerousness of criminals, among other things
- When analysing these algorithmic predictions scientifically, it is important – as it is now in the corona crisis – to reassess the relation betwen security and freedom anew. What measure of security is a basic rerquirement for freedome? And when does the former excessively curtail the latter?

that surveillance in the age of surveillance capitalism (Zuboff) becomes ever more »liquefied« (Baumann): surveillance is difficult to grasp, especially in the West, as it is no longer perceived as authoritarian force, but as realization of freedom (the digital traces we voluntarily leave in social networks come to mind). Moreover, for many citizens, whether their security fears are justified or not, it seems acceptable for them to be algorithmically evaluated as long as others are, too. This is in keeping with the naive, but effective motto: »Those who have nothing to hide have nothing to fear from algorithmic surveillance and risk evaluation!«

What remains of criminal law

Not until we comprehend what propels us toward the »criminal law« of predictive society can we arrive at the crux of the matter. What is left of our current understanding of criminal law in predictive society? What is the »criminal law« – which is intentionally put into quotation marks – of predictive society? What axioms does it rest on? And can these axioms be defended? In keeping with the best of Frankfurt traditions, we need to review the issue with a cool head without succumbing to techno phobia.

Whom, for example, does a predictive society act upon when it thinks of its members (one should no longer speak of citizens) primarily as a risk – even as potential dangers? And what effect does this have on iron principles of criminal law – such as the presumption of innocence and the in dubio pro reo principle – if the algorithmic probability calculation has precedence over the idea that judges should only convict when no reasonable doubt remains? And would this be such a terrible thing? After all, the idea of »without a reasonable doubt« is not immune to abuse either? And what does this mean with regard to the doctrine of probable cause as the necessary prerequisite for taking up criminal investigations if probable cause can visibly be generated automatically from big data? Moreover, can a democratically constituted predictive society do without the checks and balances of the law (as it is executed by humans)? (The fact that and how the Bundesverfassungsgericht – the Federal Constitutional Court – recently toppled the criminal prohibition against suicide assistance comes to mind.) Finally: can and may predictive society do without the postulate (which is admittedly not constantly realistic) that the one judging must also be able to be the one being judged (something that is difficult with algorithms)?

Do we have a right to violate the law?

But above all there is the question of freedom in the »criminal law« of predictive society. In Minority Report, a crime of passion was intentionally placed at the beginning of the story. The »criminal« (who did not even commit the crime!) was more or less spontaneously inspired to commit the »crime« (which he did not even complete!) when he found his wife in their marital bed with her lover. Crimes planned well in advance no longer exist in Minority Report. »People have gotten the message!« – is how a protagonist describes it.

What sounds like a utopia in which security (there is no more crime) and freedom (everyone enjoys legal certainty) are maximised can quickly turn into a dystopia. This happens when the getting of »the message« turns into the unavoidable internalisation of all algorithmic determinations and power structures they express; and when all criticism of the smart algorithms on the grounds of anticipatory compliance with algorithmic predictions falls silent. This is where the emancipatory and authoritarian potential of predictive society come together. And the question arises: does the autonomy to be able to in fact commit crimes belong to the core of a free democratic basic order? Is there a kind of right

The author

Christoph Burchard, 44, is Professor for Criminal Law and Criminal Procedural Law at the Faculty of Law at Goethe University, and Principal Investigator with the resesarch collaboration Normative Orders. He is a Goethe Fellow at the Forschungskolleg Humanwissenschaften Bad Homburg. Burchard's research includes changes in criminal justice through digitalisation and internationalisation, and the current renationalisation of society. In 2019 his publications included »Die Konstitutionalisierung der gegenseitigen Anerkennung« (The Constitutionalisation of Mutual Recognition) (published by Klostermann) and **»Künstliche Intelligenz als Ende des Strafrechts? Zur algorithmischen Transformation der Gesellschaft«** (Artificial Intelligence as the End of Criminal Law? On the Algorithmic Transformation of Society) (in the Jahrbuch für Recht und Ethik (Yearbook for Law and Ethics)).

burchard@jur.uni-frankfurt.de

to break the law, for example in order to initiate social change? What first seems outrageous in view of straightforward cases (manslaughter and murder), becomes clear when considering controversial cases (such as abortion, suicide assistance, consensual homosexual intercourse): A »got the message« must not make the criticism of and reflection on certain norms impossible – whether they take the form of legal provisions or algorithmically implemented programmes. This criticism and reflection requires that the individual, as an equal, is able to contribute his or her position to the making and implementation of norms. Even in predictive society, this is the only way to bring freedom and security into legitimate balance.

And now?

Minority Report ends with the Pre-Crime Programme being abandoned overnight, because a hero acting independently reveals its deficits – i.e., that predictions cannot deliver absolute certainties. The discussion of the actual »criminal law« of predictive society cannot be resolved this simply. This is why it is necessary to now place its benefits and risks under the microscope from an empirical, social scientific and normative perspective. Only then can a humane digital society be designed in which only those innovations are incorporated into the administration of criminal justice that are normatively justified and in accordance with our values. ●