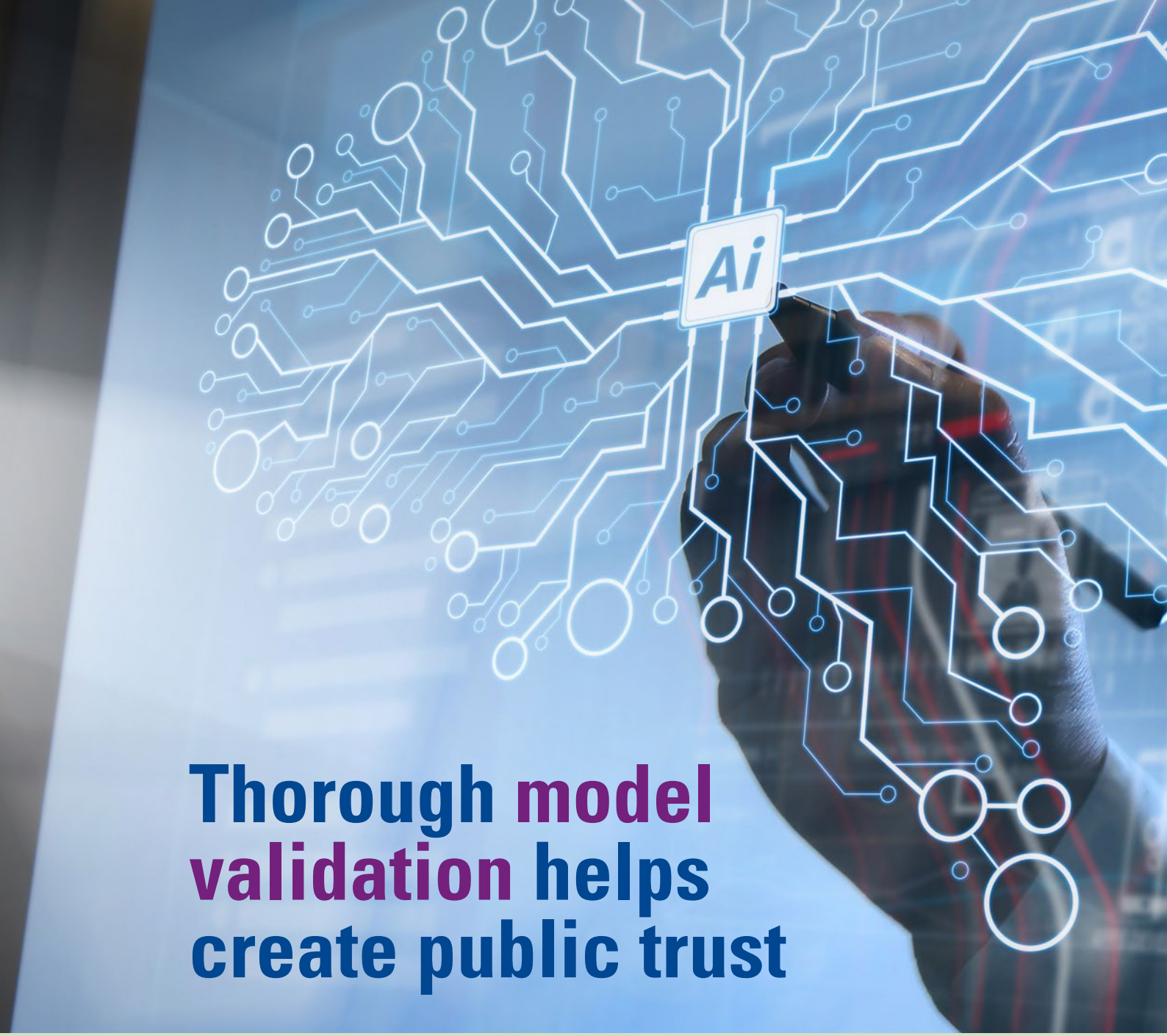

Thorough model validation helps create public trust

Performing risk analyses or detection by using algorithms may seem like a complex process, but this complexity has its origins in human decision-making. To prevent risks and negative consequences, such as unjustified bias, an independent review must be conducted. This guarantees quality and compliance with legal and ethical frameworks. KPMG has developed a method for performing independent model validations, based on a uniform assessment framework that distinguishes between four different aspects. Model validation also includes the performance of technical tests. The work to be performed and the technical tests as part of the assessment framework result in observations, findings and recommendations that the model validator reports to the organization.

INTRODUCTION

The analysis of risk by using algorithms in risk models continues to receive public attention. In terms of content, there does not seem to be agreement. Opinions differ on the very definition of a risk model, as well as on when algorithms should be used and what constitutes automated decision-making.

The problems associated with the use of risk models are regularly in the news, such as the Fraud Risk System (FSV) used by the Dutch Tax and Customs Administration. Algorithms are often referred to as "black boxes", because it is not visible why a risk model has a certain outcome. This perception logically fuels further discussion and distrust of algorithm use.

Court decisions regularly judge that risk models are not readily comprehensible. In a case concerning the System Risk Indication (SyRI), a legal instrument for combating fraud, the court ruled that the SyRI objectives are disproportionate to the additional breach of privacy. Moreover, according to the court, such a model is not sufficiently transparent ([Judi20]). Risk models and algorithms seem to be so complex that it is difficult to follow their internal logic.

COMPLEX MATTER

But where does it go wrong? It is not the algorithm or the risk model that is "wrong" per se. Human decision-making, such as selecting input data or analyzing generated signals, can also cause problems. If a risk model is elusive or complex, this is often caused by its design and set-up – i.e., by people.

> A risk model in itself is not necessarily elusive or complex

Patrick Özer MSc
is a partner at KPMG Forensic Technology.

Katja den Bieman RA LLM
is a senior manager at KPMG Forensic Investigations.

Koen van der Krogt MSc
is a manager at KPMG Forensic Technology.

Input data are data provided as input to a model. The model will generate an outcome based on these data. To teach or "train" the model, existing input data are used, where possible including the outcome: the training data. Finally, some of the pre-existing data are also kept separate to test the effectiveness of the model with different data than those used to train the model.

Developing, managing and implementing a risk model within technical, legal and ethical frameworks is a process that does not happen overnight. Recognition of the complexity of this process is key, as is identifying where that complexity stems from. This is an important step in determining how to handle a risk model. It is therefore understandable that applying and verifying risk models and algorithms is a challenge.

TAKEN FROM PRACTICE

Several examples can be found where the application of risk models goes wrong. Let's look at a few of them.

In the FSV example cited earlier, the Tax and Customs Administration used data on the dual nationality of Dutch citizens as an indicator in the system that automatically labeled certain applications for childcare benefits as high-risk. Both KPMG and the Dutch Data Protection Authority found after an investigation that the Tax and Customs Administration wrongfully retained these sensitive data for years and made unlawful use of a "black list" ([KPMG20], [DDPA20], [DDPA21]).

A second example concerns the municipality of Rotterdam, which uses an algorithm to assign individuals a risk score to predict welfare fraud. In December 2021, the Rotterdam Court of Audit cautioned that input factors such as gender and residential area were possibly used to determine this risk. This could make the risk model unethical. In response to the Court of Audit's investigation, SP (Socialist Party) member Renske Leijten submitted parliamentary questions about the use of algorithms by local governments. Minister of the Interior and Kingdom Relations Hanke Bruins Slot decided not to commission an investigation at the central level, partly in view of the fact that the responsibility for investigations lies with the municipalities themselves, not with the national government ([Team22]). The algorithm register published by the municipality of Rotterdam still refers to the risk assessment model used with regard to benefit irregularities, stating that the algorithm does not process data that could lead to discrimination ([Muni22]).

In addition to examples from the Netherlands, there are international examples. International government agencies and judicial institutions also use risk models. The US First Step Act was introduced in 2018 under the Trump administration. The purpose of this act was to shorten unnecessarily long sentences. Based on the PATTERN risk model, prisoners are given the opportunity to win early release if they have a low probability of relapsing into criminal behavior. Civil rights groups were quick to express concerns about possible disproportions based on race. The algorithm was said to assess the likelihood of recidivism significantly higher if someone had an African-American, Hispanic, or Asian background ([FBP22]). Involving a person's criminal history as a risk factor may be problematic because ethnic profiling is a well-known issue in the US. The additional inclusion of education as a risk factor may have an indirect reinforcing effect. The risk model is still used and can be found on the Federal Bureau of Prisons site ([John22]).

The above examples illustrate the risks and undesirable consequences associated with the use of questionable algorithms in risk models. The examples also show the need for independent validation of such risk models to enforce due diligence in the use of algorithms and predictive models.

POOLING KNOWLEDGE

Input of sufficient substantive knowledge is a requirement to properly apply and validate risk models and algorithms. This knowledge has a number of aspects:

- Domain knowledge about the scope is required to determine whether the risk model's objective is feasible and how this objective can be achieved. In addition, domain knowledge is required to determine the necessary data, hypotheses and prerequisites, and ultimately to verify that the results of the model are correct.
- Technical knowledge is needed to determine the most appropriate type of algorithm for the risk model, to develop an algorithm for a risk model, to analyze the often large quantities of data, and for final programming.
- Legal knowledge is needed for the legal frameworks that directly apply to the model and its use, as well as for the legal frameworks and guidelines in the area of data privacy and human rights. By extension, knowledge about the ethical frameworks is relevant with respect to the prevention of possible discrimination or bias.

The pooling of all this knowledge in the development and management of a model or algorithm is critical in determining whether a model can be applied.

BIAS IN RISK MODELS

Bias and the prevention of discrimination is a hotly debated topic in the application of risk models and algorithms. *Bias* is a distortion of research results, a preconception that can get in the way of an objective observation or assessment. Another concept that is often included is *prejudice*, where a judgment is made without having examined all the facts. Society is justifiably critical of this subject. An important point to take into account in the public debate and during the development of models is that bias is always part of a risk model or algorithm to some extent. The reason is that bias does not always have to be direct; it can also be indirect. Indirect bias means that a characteristic that itself does not contain direct bias is related to a characteristic that does contain bias. For example, the length of a resume is related to a person's age, and the zip code of a person's home address may be related to their level of education, ethnicity or age. For almost every characteristic there is a related characteristic where there is bias. This does not mean, however, that risk models are by definition discriminatory, but it does mean that consideration must be given to possible bias and the ethics involved in applying the model and the effect of bias. This already starts in the step of determining which criteria will or will not be included in a risk model. It is important to recognize and record this direct and indirect bias during the development of a risk model so that the influence and use of this information in an algorithm can be intentionally accepted or mitigated.

REVIEWING RISK MODELS

To ensure that the right knowledge is used in the development of a risk model and that bias is adequately taken into account, it is important to establish effective frameworks within which to act. Establishing the frameworks of a risk model or algorithm is an important step in assessing whether a model or algorithm can be applied and will still be appropriate later on. For this assessment, it is useful to look at the risk model from a fresh perspective. An independent review of a risk model or algorithm to support the judgment is an effective tool to make a solid decision to start using a risk model.

REVIEW FRAMEWORKS

The frameworks to be reviewed may include hard requirements, such as "Has a Data Privacy Impact Assessment (DPIA) been performed?" or "Have all personal data used been documented?", but also less rigid requirements, such as "Is the type of algorithm chosen appropriate for our specific purpose?". Reviewing these frameworks requires the professional judgment of an auditor or validator. This makes an independent review – also called quality control or model validation – complex but at least as important as the risk model development process. Therefore, it is important that an auditor or validator has knowledge of and experience with the development and verification of models and algorithms, the scope and the legal and ethical frameworks.

Frameworks for the application or verification of risk models or algorithms are also the subject of public debate. The following guidelines have emerged from this:

- In 2021, the Ministry of the Interior and Kingdom Relations released the Impact Assessment for Human Rights in the Deployment of Algorithms (IAMA) ([MIKR21]). This considers the choice of applying algorithms and the responsible development and implementation.
- The Court of Audit released an assessment framework ([CoAu21]) for quality control of algorithms in 2021 and applied it to nine algorithms used by government ([NCoA22]).
- NIST is working on an AI Risk Management Framework, which will be published in late 2022, early 2023. A draft version is already available ([NIST22]).
- NOREA has also published a set of principles for examining algorithms ([NORE21]).
- The US offers guidelines from the Office of the Comptroller of the Currency (OCC) on Model Risk Management ([OCC21]), which have been applied to financial and compliance risk models for many years in the financial world.

It is important to establish effective frameworks within which a risk model should be developed

These documents provide valuable information for establishing frameworks for the development of models and algorithms and their verification or validation.

METHOD FOR MODEL VALIDATION

We believe that an independent review must be conducted to safeguard the quality and compliance with legal and ethical frameworks of a risk model and its intended use. Therefore, KPMG has developed a method for conducting independent model validations, based on existing frameworks and knowledge of and experience with performing model validations in different sectors.

A model validation should look at several aspects that together form the context of the risk model. The governance of a risk model provides insight into arranged roles and responsibilities. As part of governance, the objective of the risk model – in the larger context of an organization – should also be established, because a risk model should not be completely isolated. Based on this set-up, the concept of the risk model can be developed and embodied in a technical design. The conceptual model and the technical design must show whether the set-up is in accordance with the initial objective. The next step is to analyze whether not only the set-up but also the technical functioning of the risk model fits the objective formulated. It is possible, for example, that a risk model does have predictive value, but based on a different hypothesis than was intended. If the risk model functions as intended, the final component is the periodic evaluation of and accountability for the risk model. Here, too, it is important to recognize that a risk model must fit within its context and take into account changing circumstances such as new laws and regulations or changes in input data over time, so-called "data drift".

Based on the above, we have set up an assessment framework that covers four aspects:

1. Governance and design;
2. Conceptual model and technical design;
3. Functioning of the risk model;
4. Evaluation and accountability.

A more detailed description of these aspects follows below. To make it concrete, examples of work to be performed are also included for the specific aspect.

GOVERNANCE AND DESIGN

In the "Governance and design" aspect, the development of a risk model is assessed against relevant legislation and regulations and other prevailing systems of standards. For example, it is examined whether the objective of the risk model has been clearly formulated and whether the work was performed within the relevant legal and ethical frameworks. This is the basis of the risk model. Also relevant is whether the risk model does not overshoot itself and whether the development of a risk model is appropriate to the objective it is intended to pursue. Have proportionality (the means used must be in proportion to the objective to be achieved) and subsidiarity (the means used must be the least onerous means of achieving the objective) been sufficiently weighed? In other words: can the purpose of the risk model also be effectively achieved through risk selection with fewer personal data or with less privacy-intrusive or alternative means? Also important is the design of the governance structure for the risk model. It must be clear who bears which responsibilities from which role at various levels within the organization – from project team to management. One question the model validator needs to answer is whether there is sufficient knowledge in the organization based on the defined roles and responsibilities, whereby the number of years of relevant experience or relevant education plays a role. This may lead to the conclusion that there is sufficient or too little expertise in the team using the risk model. It is also important to carry out a thorough risk analysis prior to development.

For this aspect, the model validator also looks at the DPIA. This is relevant to gain insight into evaluations in place within the organization based on identified and described legal guidelines and to prevent bias and discrimination. The considerations concerning the ethical frameworks and the risk analysis must have been documented during the development of a risk model.

An example of non-compliance with legal frameworks on DPIAs, from March 2022, is a dispute between the Internet Covert Operations Program (iCOP) operated by package delivery company USPS and the Electronic Privacy Information Center (EPIC). iCOP deployed facial recognition to identify potential threats while monitoring social media posts. The use of such facial recognition raises significant risks and ethical concerns, and in addition, EPIC said the program used would be illegal due to the lack of a DPIA ([Hawk22]).

CONCEPTUAL MODEL AND TECHNICAL DESIGN

With respect to the aspect "Conceptual model and technical design", the model validator performs activities to validate that the conceptual model and technical design are in line with the objective of the risk model and the associated frameworks as identified in

the aspect "Governance and design". In doing so, the model validator analyzes the availability and quality of the description of the conceptual model and technical design in documentation. The model validator tests the clarity and explainability of the description and underlying assumptions.

This aspect includes identifying a description and justification of the assumptions and choices underlying the technical design. There must be sufficient justification for the training data, algorithms and programming language chosen to develop the risk model.

A relevant component for this aspect is the use of variables with indirect bias. An example showing that the prevention of indirect bias is not always given sufficient attention relates to the success rate of applicants at e-commerce company Amazon. In 2015, machine learning specialists at Amazon discovered that the algorithm developed for selecting new candidates was biased. The algorithm observed patterns in resumes submitted over a ten-year period. Given the male dominance in the tech industry, the algorithm taught itself to favor resumes from men – based on history. If a resume contained words such as "women" or "captain of the women's chess club", the candidate was removed from the list of candidates ([Dast18], [Logi19]).

FUNCTIONING OF THE RISK MODEL

Activities under the review aspect "Functioning of the risk model" are focused on reviewing whether the functioning of the risk model matches the objective and the design of the risk model from the previous two aspects. Has the design been translated correctly into the technical implementation and does the risk model produce the results as intended?

The model validator analyzes as part of this aspect whether technical tests were performed in the development of a risk model to assess the functioning and output of the model. In doing so, the model validator must analyze which tests were performed and what the results were. In addition, the model validator checks whether tests have been performed to check the quality of the input data and whether there is proper version control. The model validator also performs independent technical tests (see the subsection below).

Also relevant to this aspect is a review of the description of the programmed risk model. Here, at least a number of points must be sufficiently explained, such as an overview of the input used, the functioning of the risk model, the algorithm applied, any uncertainties and limitations, and an explanation of why the risk model is suitable for its intended use.

> An independent review must be conducted to ensure the quality of a risk model

A possible finding of the model validator regarding this aspect may relate to the quality of the data used. If the training data are of poor quality, this will probably mean that the quality of the generated results is also below par. An example of this is an algorithm used by the Dutch Railways (NS). A customer was unable to purchase a subscription because the zip code of applicants was used as input for their credit check. If, as in this case, it turned out that a former resident of the address was a defaulter, the customer received a negative credit score and the application was denied ([Voll22]).

Technical tests

Part of our methodology includes a technical test of the risk model. One of the technical tests we use to validate whether the technical implementation of the risk model matches the conceptual model and the technical design is a code review. This involves – partly automated and partly manual – reviewing the programmed code in detail and "re-performing" it to verify that it matches the design and generates the intended results.

In addition, stability tests can be performed. In this process, the model validator re-runs the programmed code of the risk model several times with the same and minimally adjusted input data to analyze their impact on the results. The input data can also be adjusted with extreme values to determine the impact of these extreme values on the risk model and whether they were handled properly. The purpose is to verify that the risk model is sufficiently stable.

Finally, performance tests can be conducted to determine whether the model is sufficiently effective in "predicting" the intended outcomes.

EVALUATION AND ACCOUNTABILITY

Under the aspect "Evaluation and accountability", the model validator specifically tests that the model is used in accordance with the objective and guidelines. The model validator also tests the organization's evaluation mechanism, including an analysis of how accountability is provided. This aspect is the culmination of the previous three aspects and looks back at the various elements described earlier.

Part of this aspect is a "layman's test": are the results of the risk model logical, viewed from the perspective of a relatively uninformed person? This concerns the comprehension of the logic of the risk model's ourcomes for uninvolved people and acts as a mirror. The model validator analyzes whether the results generated are to be expected based on logical reasons, what possible explanations there may be for deviations, and whether the outcomes are explainable. It is a test with a helicopter view: is, all things considered, the risk model sufficiently understandable?

Within this aspect, the model validation simultaneously considers whether (in the documentation) any recommendations from performed tests and previous evaluations have been followed up and whether the use and future use of the risk model are described.

An existing risk model where safeguarding of the intended use can be questioned concerns the algorithms behind the determination of the credit scores of individuals at banks in the US. The impact of an overdue payment on the credit score is greater for customers with higher (generally "better") credit scores than for those with lower credit scores. This effect is caused by the underlying algorithm: when someone has a higher score, this score is more sensitive to negative events, which means that the same event can have a different impact on different individuals ([Sing22]).

CAN A RISK MODEL BE USED?

Our starting point for each model validation is a uniform assessment framework based on the above aspects. The assessment framework forms the basis for performing the model validation. It is important that the model validator maintain a professional-critical attitude.

The assessment framework provides the model validator with observations and findings to report to the organization. In doing so, the model validator may make recommendations, where necessary. The model validator's report is a sound basis for determining whether a risk model can and may be put into use.

It is all about the relationship between people and technology

CONCLUSION

As is so often the case, it is all about the relationship between people and technology. Did the developer set up a suitable process to arrive at an appropriate risk model? Was thorough risk analysis, broader than just a DPIA, conducted prior to the development of the risk model? Does the technology match the design, by human beings, and does the risk model deliver the intended results? These and other important questions that arise during the process of developing a risk model, and the technical risk model itself, have been incorporated into an independent review.

Whether it is called an independent review, quality control or model validation – they all refer to the same activity. KPMG has developed this method for the systematical validation of risk models, from the creation process, the technique, to the outcomes. The method was developed on the basis of the IAMA, the assessment framework of the Dutch Court of Audit, the OCC Model Risk Management guideline and more than ten years of experience in performing model validations in various sectors. KPMG has been using this method for four years.

Unfortunately, as noted at the beginning of this article, risk models do not always function as intended. This damages public trust to such an extent that the benefit of using a risk model – increased effectiveness and efficiency – is quickly canceled out. This is despite the fact that the risk model should actually contribute to public trust, partly because it should be more objective than a completely manual assessment. However, the technology of a risk model or algorithm is also based on human decision-making; it is a good thing that thorough checks and balances are in place to achieve the most reliable joint performance of man and machine.

References

[Boer21] Boer, A., & Van Meel, M. (2021). Algoritmes en mensen moeten blijven leren. KPMG. Retrieved from: https://home.kpmg/nl/nl/home/insights/2021/06/algoritmes-en-mensen-moeten-blijven-leren.html

[CoAu21] Court of Audit (2021, 26 January). *Aandacht voor algoritmes*. Retrieved from: https://www.rekenkamer.nl/publicaties/rapporten/2021/01/26/aandacht-voor-algoritmes

[Dast18] Dastin, J. (2018, 11 October). Amazon scraps secret AI recruiting tool that showed bias against women. *Reuters*. Retrieved from: https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

[DDPA20] Dutch Data Protection Authority (2020, 17 July). Werkwijze Belastingdienst in strijd met de wet en discriminerend. Retrieved from: https://autoriteitpersoonsgegevens.nl/nl/nieuws/werkwijze-belastingdienst-strijd-met-de-wet-en-discriminerend

[DDPA21] Dutch Data Protection Authority (2021, 7 December). Boete Belastingdienst voor discriminerende en onrechtmatige werkwijze. Retrieved from: https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/boete-belastingdienst-voor-discriminerende-en-onrechtmatige-werkwijze#:%7E:text=In%20de%20zomer%20van%202020,de%20bestrijding%20van%20georganiseerde%20fraude.

[FBP22] Federal Bureau of Prisons (n.d.). BOP: First Step Act, Resources. Retrieved from: https://www.bop.gov/inmates/fsa/pattern.jsp

[Hawk22] Hawkins, S. (2022, 29 March). USPS Escapes Claims Over Its Facial Recognition Technology. *Bloomberg Law*. Retrieved from: https://news.bloomberglaw.com/tech-and-telecom-law/usps-escapes-claims-over-its-facial-recognition-technology

[Hiji22] Hijink, M. (2022, 12 January). Wie zet z'n tanden in de foute algoritmes? *NRC*. Retrieved from: https://www.nrc.nl/nieuws/2022/01/12/wie-zet-zn-tanden-in-de-foute-algoritmes-a4077972

[John22] Johnson, C. (2022, 26 January). Flaws plague a tool meant to help low-risk federal prisoners win early release. *NPR*. Retrieved from: https://choice.npr.org/index.html?origin=https://www.npr.org/2022/01/26/1075509175/justice-department-algorithm-first-step-act?t=1650375204324&t=1652358333950

[Judi20] The Judiciary (2020, 5 February). SyRI-wetgeving in strijd met het Europees Verdrag voor de Rechten voor de Mens. Retrieved from: https://www.rechtspraak.nl/Organisatie-en-contact/Organisatie/Rechtbanken/Rechtbank-Den-Haag/Nieuws/Paginas/SyRI-wetgeving-in-strijd-met-het-Europees-Verdrag-voor-de-Rechten-voor-de-Mens.aspx

[KPMG20] KPMG Advisory N.V (2020, 10 July). *Rapportage verwerking van risicosignalen voor toezicht: Belastingdienst*. Retrieved from: https://open.overheid.nl/repository/ronl-42970d17-d8b9-41d6-aa8f-docc52ab97c8/1/pdf/kpmg-rapport-fsv-onderzoek-belastingdienst.pdf

[Logi19] Logically (2019, 30 July). 5 Examples of Biased Artificial Intelligence. Retrieved from: https://www.logically.ai/articles/5-examples-of-biased-ai

[MIKR21] Ministry of the Interior and Kingdom Relations (2021, July). *Impact Assessment Mensenrechten en Algoritmes*. Retrieved from: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/25/impact-assessment-mensenrechten-en-algoritmes

[Muni22] Municipality of Rotterdam (2022). Algorithm register. Retrieved from: https://www.rotterdam.nl/bestuur-organisatie/algoritmeregister/

[NCoA22] Netherlands Court of Audit (2022, 18 May). *Algoritmes getoetst*. Retrieved from: https://www.rekenkamer.nl/publicaties/rapporten/2022/05/18/algoritmes-getoetst

[NIST22] National Institute of Standards and Technology (2022). NIST Artificial Intelligence Risk Management Framework (AI RMF). Retrieved from: https://www.nist.gov/itl/ai-risk-management-framework

[NORE21] NOREA (2021, December). *NOREA Guiding Principles Trustworthy AI Investigations*. Retrieved from: https://www.norea.nl/download/?id=10966

[OCC21] Office of the Comptroller of the Currency (2021, 18 August). Model Risk Management: New Comptroller's Handbook Booklet. *OCC Bulletin* 2021-39. Retrieved from: https://www.occ.treas.gov/news-issuances/bulletins/2021/bulletin-2021-39.html

[Pols21] Pols, M. (2021, 15 December). Privacywaakhond AP krijgt nieuwe taak als algoritmetoezichthouder en meer geld. *FD.nl*. Retrieved from: https://fd.nl/bedrijfsleven/1424029/privacywaakhond-ap-krijgt-nieuwe-taak-als-algoritmetoezichthouder-en-meer-geld-nle2cacLRhoP

[Sing22] Singer, M. (2022, 22 March). How To Guard Against Sudden, Unexpected Drops In Your Credit Score. *Forbes*. Retrieved from: https://www.forbes.com/sites/theyec/2022/03/22/how-to-guard-against-sudden-unexpected-drops-in-your-credit-score/?sh=2f89893e6bf5

[Team22] Team Stadszaken.nl (2022, 21 March). BZK: gemeenten moeten zelf bepalen hoe ze met algoritmes omgaan. *Stadszaken.nl*. Retrieved from: https://stadszaken.nl/artikel/4169/bzk-gemeenten-moeten-zelf-bepalen-hoe-ze-met-algoritmes-omgaan

[Voll22] Vollebregt, B. (2022, 18 January). Zo werd Myrthe Reuver de dupe van haar data: 'Ze geloven in eerste instantie het systeem'. *Trouw*. Retrieved from: https://www.trouw.nl/economie/zo-werd-myrthe-reuver-de-dupe-van-haar-data-ze-geloven-in-eerste-instantie-het-systeem~b17af53f/

[VVD21] VVD, D66, CDA and ChristenUnie (2021, 15 December). *Omzien naar elkaar, vooruitkijken naar de toekomst: Coalitieakkoord 2021 – 2025*. Retrieved from: https://www.kabinetsformatie2021.nl/documenten/publicaties/2021/12/15/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst

About the authors

Patrick Özer MSc is a partner at KPMG Forensic Technology and is responsible for the Forensic Technology team. He is involved in fraud- and compliance-related projects in various sectors, focusing on conducting digital forensics and combating financial-economic crime. As part of this, he focuses on compliance- and risk model validation.

Katja den Bieman RA LLM is a senior manager at KPMG Forensic Investigations. As a forensic accountant, she is mainly concerned with fraud prevention as part of fraud risk management and with fraud response from (person-oriented) fact-finding into financial administrations, processes and behaviors. She is specialized in forensic services to the public sector.

Koen van der Krogt MSc is a manager at KPMG Forensic Technology. He focuses on digital investigation and (forensic) data analytics and specializes in validating models and systems for compliance. He helps clients to get quick insights into large amounts of data and facilitates smooth and efficient reviews and investigations.