E

n *Journal Of Governmental & Nonprofit Accounting*, de *American Accounting Association*, Vol. 10, No. 1, pp. 26–49, encontramos el artículo [Integrated Business Intelligence and Analytics: The Case of the Department of the Navy](file:///C:\Users\hdobe\Dropbox\Mi%20PC%20(LAPTOP-SSPTUC37)\Documents\hbg\borradorescontrapartida\10.2308\JOGNA-17-001,%202021), escrito por Robert J. Eger III & Christy Smith, quienes concluyeron: “*Through the use of established data analytics techniques currently employed in the commercial sector, addressing the issue of fraud with the implementation of BIA software and hardware aids in detecting anomalies associated with fraud schemes. The detection of these anomalies raises red flags within the processes of multiple stakeholders, sparking a further proactive investigation into the underlying cause of the red flag. Data analytics software allows for the near-instantaneous analysis of vast amounts of data that would have previously sat dormant, thereby enabling fraud scheme detection within government processes, and it provides the flexibility to detect previously unknown fraud schemes. ―Our stakeholder interviewees imply that by using a data analytics software program in the prevention of fraud, the critical resources of money, manpower, and time could be protected from fraudulent activities in a proactive manner. This proactive approach identifies fraudulent activities before they are carried out and reduces costs to the taxpayers associated with lost resources due to fraud. These critical resources can then be available for more efficient use. ―We acknowledge that our findings are just the beginning of the needed research into the practicality of a specific data analytics program implementation across the entire U.S. Department of Defense (DoD), not only our focus on the U.S. Navy. The DoD is an expansive organization that utilizes vast amounts of resources with many organizations that span across its agencies. A data analytics program that focuses on fraud would be most beneficial if it used all sources of available data generated by the DoD.*” Observamos, en primer lugar, que hay muchas similitudes entre las empresas públicas gubernamentales y las privadas. El marco jurídico es bastante diferente pero no así su comportamiento económico y administrativo. En segundo lugar, debido a nuestro conocimiento de herramientas para manejar y analizar grandes datos, aceptamos sin reservas la conclusión, porque estamos seguros que con ellas se pueden advertir previamente posibles actos fraudulentos, sin efectos importantes en los procedimientos o en la intervención del personal. Hay que tener un gran conocimiento de los datos, para saber cuáles datos buscar, que características se deben comprobar y cuándo se tienen que realizar las pruebas. Sin este conocimiento la herramienta no arrojará datos útiles. De las malas programaciones solo se obtiene basura. Como se deduce rápidamente, los fraudes que aparentan operaciones normales serán más difíciles de identificar. Por eso deben comprobarse otros extremos, como la integridad de los registros, la existencia de los activos y pasivos y la ocurrencia de los ingresos y las erogaciones, aspectos que en muchos casos implican procedimientos de inspección, observación o documentación, que permitan concluir si los registros corresponden a hechos económicos reales. Estamos ante un escenario lleno de astutos.

*Hernando Bermúdez Gómez*